

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2002 年 10 月 31 日 (31.10.2002)

PCT

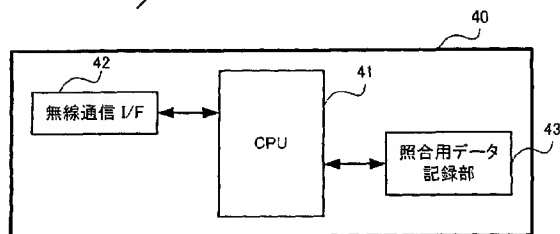
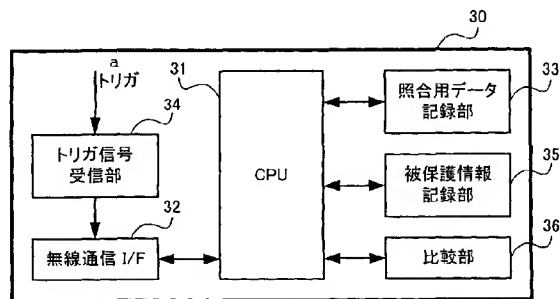
(10) 国際公開番号
WO 02/086808 A1

- (51) 国際特許分類: G06K 17/00, 19/073, G06F 12/14, 15/00, H04Q 7/38
- (21) 国際出願番号: PCT/JP02/03789
- (22) 国際出願日: 2002 年 4 月 17 日 (17.04.2002)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ: 特願2001-118795 2001 年 4 月 17 日 (17.04.2001) JP
- (71) 出願人: 株式会社モビリティ (MOBILITY CO., LTD.) [JP/JP]; 〒105-0001 東京都港区虎ノ門1丁目16番9号 Tokyo (JP).
- (72) 発明者: 榊原 辰彦 (SAKAKIBARA, Tatsuhiko); 〒105-0021 東京都渋谷区恵比寿西2丁目8番5号 高麗羅
- (74) 代理人: 鈴木 正剛 (SUZUKI, Seigoh); 〒105-0014 東京都港区芝三丁目2番7号 芝Nビル4階 Tokyo (JP).
- (81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GI, GM, GR, GU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MY, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.
- (84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許

[続葉有]

(54) Title: INFORMATION PROTECTIVE SYSTEM AND INFORMATION PROTECTIVE METHOD

(54) 発明の名称: 情報保護システム及び情報保護方法



a...TRIGGER
34...TRIGGER SIGNAL RECEIVING UNIT
32...RADIO COMMUNICATION I/F
33...INQUIRY DATA RECORDING UNIT
35...PROTECTED INFORMATION RECORDING UNIT
36...COMPARING UNIT
42...RADIO COMMUNICATION I/F
43...INQUIRY DATA RECORDING UNIT

(57) Abstract: Authentication is given when first and second devices (30, 40) close to each other communicate with each other in a noncontact way, and the protected information (35) in the first device (30) is made accessible externally. After a cellular telephone (300) is brought close to a cap (400) to gain authorization, the cellular telephone (300) serving as a ticket can pass through a ticket gate.

[続葉有]



(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:

— 国際調査報告書

(57) 要約:

第1の装置(30)と第2の装置(40)とが近傍において非接触通信を行って認証を得ることにより、第1の装置(30)内の被保護情報(35)に外部からアクセス可能となる。

携帯電話(300)と帽子(400)とを近接させて認証を得た後に、携帯電話は乗車券として改札機を通過できる。

明細書

情報保護システム及び情報保護方法

技術分野

- 5 本発明は無線通信を利用した情報保護技術に関するものである。

発明の背景

近年、市場には膨大な数の磁気カードが流通している。一例として、クレジットカード、キャッシュカード、プリペイドカード、社員証や学生証、通行証、各種証明書発行用カード、図書館の貸出カード、入退室管理カードなどがあげられる。これらのカードは特定の目的ごとに提供されているため、場合によっては外出時に何枚ものカードを携帯しなければならない。しかしながら、カードの枚数によっては非常にかさばる上に、必要なときに必要なカードをすぐに取り出しにくいなどの問題がある。

- 15 これに対する対応策として、複数のカードを可能な限り 1 枚にまとめる方法が考えられる。たとえば、金融機関のキャッシュカードをクレジットカードとしても利用できるようにしたカードが、デビットカードとして実用化されている。デビットカードの所有者は、店舗備え付けの端末にカードを挿入して暗証番号を入力するだけで、現金を持ち歩かずに商品を購入することが
20 できる。

- しかしながら、決済時にテンキーを使って自分で暗証番号を入力しなければならず、暗証番号漏洩の不安を拭いきれないことが普及の妨げとなっている。また、デビットカードでは磁気ストライプを利用しているため、紛失や盗難事故の際に改竄されやすいという問題もある。事実、磁気ストライプに
25 記録されたデータを読み取り、偽造カードにコピーして使用する「スキミング」と呼ばれる被害が近年になって急増している。

こうしたカードの改竄や不正使用が増えている現状を背景に、磁気カードから IC カードに切り替える動きが各業界において本格化しつつある。周知のように、IC カードとはプラスチック製のカードに IC チップを埋め込ん

だもので、磁気カードに比べて偽造が難しいという利点がある。また、データ記録容量が極めて大きいため、複数のカードを1枚にまとめた多目的カードを比較的容易に製造することができるという利点もある。

しかしながら、従来のクレジットカードなど個人情報と金銭的価値の両方が付帯するカードの場合、所有者以外の第三者に不正使用された場合の被害は甚大である。一方、金銭的な価値がありながら匿名性の高いカード（プリペイドカードなど）では、紛失や盗難事故の際に所有者の手元に戻ってくる可能性が極めて低いという欠点がある。さらに、金銭的な価値はなくとも個人情報が多く記録されたカード（住民カードや保健医療カードなど）であればプライバシー保護の観点からさまざまな問題が危惧される。

そこで、携帯電話、PHS、携帯情報端末（PDA）、ノートパソコンなどの携帯端末に多目的ICカードを統合したり、複数のICカードの機能を搭載したり、あるいは搭載可能な仕組み（ICカードとしての機能を実行するためのソフトを所定のサーバ等にダウンロード可能な形態で提供し、そのソフトをダウンロードする、あるいはこのようなソフトが搭載された、カード用専用チップを装着する等）を用意するなどし、この端末に対してセキュリティ対策を施す方法が検討されている。ICカードには大きく分けて接触型と非接触型の2種類があり、カードに記録されたデータを利用するには接触型の場合は専用の端末（以下、「リーダライタ」と呼ぶ）にカードを挿入しなければならないが、非接触型ではその必要がなく、リーダライタにかざすだけでよい。したがって、携帯端末をパスワードで保護し、端末にあらかじめ記録されたパスワードと所有者が入力するパスワードとが一致した場合にのみICカードの機能を利用できるようにする方式が考えられる。しかしながら、このような方式ではカード機能を利用するたびに端末にパスワードを入力しなければならない煩わしさがああり、リーダライタにかざすだけでよいという非接触型ICカードの利点が半減してしまう。また、パスワード自体は所有者個人を特定する手段にはならず、何らかの理由でパスワードが漏洩した場合に、悪意の拾得者が不正入手したパスワードを利用して端末にアクセスする可能性もある。

あるいは、携帯端末の紛失時に通常の電話機を利用して遠隔地から携帯端末を緊急制御する方法も考えられる。すなわち、プッシュボタン操作によって生成される信号を利用して携帯端末の不正使用を防止するものである。しかしながら、この方法では遠隔操作に対応した基地局の存在が不可欠になるため、確実に不正使用を防止するという意味では不十分である。

- 本発明は上記課題に鑑みてなされたものであり、その目的とするところは、個人情報や金銭的価値のある情報を統合して管理する場合に当該情報の第三者による不正使用を確実に防止するための情報保護システムを提供することにある。
- 本発明の他の目的は、かかる情報保護システムを実現するための情報保護方法を提供することにある。

発明の開示

- 本発明の一形態に係る情報保護システムは、被保護情報が記録された第 1 アセンブリと、認証情報が記録された第 2 アセンブリとを含む情報保護システムであって、前記第 2 アセンブリは前記第 1 アセンブリからの要求に応じて非接触による情報の送信を可能にする通信手段を備えるものであり、前記第 1 アセンブリは、前記被保護情報に対するアクセスを受け付ける受付手段と、前記認証情報を前記第 2 アセンブリより受け取って認証を行う認証手段と、この認証手段による認証結果に応じて前記受付手段で受け付けたアクセスを許可又は禁止するアクセス制御手段とを備えるものである。

- また、本発明の他の形態に係る情報保護システムは、その所有者を認証するための第 1 認証情報と被保護情報とが記録された第 1 アセンブリと、前記所有者を認証するための第 2 認証情報が記録された第 2 アセンブリと、前記被保護情報を読み取る情報読取装置とを含む情報保護システムであって、前記第 1 アセンブリは、前記第 2 アセンブリおよび情報読取装置との間で非接触による情報の送受信を可能にする第 1 通信手段を備えるものであり、前記第 2 アセンブリは、前記第 1 アセンブリとの間で非接触による情報の送受信を可能にする第 2 通信手段を備えるものであり、前記情報読取装置は、前記第

1 アセンブリとの間で非接触による情報の送受信を可能にする第3通信手段を備えるものであり、前記第1アセンブリは、さらに、前記情報読取装置からの信号に応答して前記第2アセンブリより前記第2認証情報を受け取り、受け取った第2認証情報および前記第1認証情報に基づく認証を行い、
5 認証結果に応じて前記被保護情報の前記情報読取装置による読み取りを許可又は禁止する手段を備えるものである。

本発明の一形態に係る情報保護システムにおいては、認証手段を第2アセンブリ、又は、第1アセンブリと第2アセンブリとの双方に設けても良い。これらの第1アセンブリ、第2アセンブリは、いずれも、単独で携帯可能であるか、または携帯可能な製品に内蔵された形態で提供することが可能である。
10

前記通信手段における通信形態には特に制限はない。例えば、前記通信手段は、電磁誘導による無線通信、電磁結合による無線通信、静電結合による無線通信、マイクロ波帯の周波数を用いた無線通信、及び光を情報の搬送媒体とする通信、のいずれかによって通信を行う構成とすることができる。
15

また、前記第1アセンブリおよび前記第2アセンブリを、それぞれ非接触通信用のアンテナを含むICモジュールとして提供してもよい。

前記第1アセンブリの形態としては、カード媒体に埋め込まれた形態、シート状の媒体に埋め込まれた形態、携帯性端末に内蔵された形態、データキャリアに内蔵された形態等が挙げられる。
20

前記第2アセンブリは、好適には、前記第1アセンブリを所持する者が常に持ち歩くもの、より好適には第3者が容易に盗むことができないものとする。例えば、前記第1アセンブリを、所持する者が身につける装飾品、例えば指輪に埋め込むことができる。

25 また、本発明の他の形態では、前記アクセス制御手段は、当該認証手段でアクセスを許可するという認証結果が得られた場合は、前記アクセス要求から所定時間が経過するまでは、被保護情報へのアクセスを許可する。

また、第1、第2のアセンブリは、集積回路アセンブリとして提供することも可能である。

図面の簡単な説明

図 1 は、本発明の一実施形態による情報保護システムの概要を示すブロック図である。

- 5 図 2 は、I C アセンブリ 3 0 へのアクセス要求に対しての I C アセンブリ 3 0 の C P U 3 1 における認証処理を表すフローチャートである。

図 3 は、多目的携帯端末 3 0 0 と R バッジ 4 0 0 の説明図である。

図 4 は、自動改札機に非接触型 I C カード用のリーダライタ 5 0 を設けた例の説明図である。

- 10 図 5 は、R F I D インターフェースを備えた携帯端末の構成を表す図である。

図 6 は、複数の R F I D インターフェースを備えた携帯端末の構成を表す図である。

図 7 は、携帯端末のソフトウェアの構成を表す図である。

- 15 図 8 は、I C カードの構成を表す図である。

図 9 は、電磁誘導による送受信の仕組みを示す図である。

図 1 0 は、データを受信の動作を表すフローチャートである。

図 1 1 は、データを発信の動作を表すフローチャートである。

図 1 2 は、個別情報システムの構成を表す図である。

- 20 図 1 3 は、携帯端末に個別情報が格納されているようすを示す図である。

図 1 4 は、個別情報システムの動作を示すフローチャートである。

図 1 5 は、使用者識別システムの構成を表す図である。

図 1 6 は、レッドバッジの例を表す図である。

図 1 7 は、レッドバッジの例を表す図である。

- 25 図 1 8 は、レッドバッジの例を表す図である。

図 1 9 は、レッドバッジの I C チップの構成を表す図である。

図 2 0 は、識別情報を登録する動作を表すフローチャートである。

図 2 1 は、識別情報より利用可能かを判断する動作を表すフローチャートである。

図 2 2 は、レッドバッジを個別情報システムで利用した図である。

図 2 3 は、携帯記録素子書込システムの構成を表す図である。

図 2 4 は、携帯記録素子書込システムの動作を示すフローチャートである。

図 2 5 は、携帯記録素子書込システムでレッドバッジを利用した図である。

5 図 2 6 は、管理システムの第 1 の構成を表す図である。

図 2 7 は、利用管理システムの第 1 の動作を表す図である。

図 2 8 は、携帯端末に表示される画面の例である。

図 2 9 は、第 1 の利用管理システムでレッドバッジを利用した図である。

図 3 0 は、利用管理システムの第 2 の構成を表す図である。

10 図 3 1 は、利用管理システムの第 2 の動作を表す図である。

図 3 2 は、携帯端末に表示される画面の例である。

図 3 3 は、第 2 の利用管理システムでレッドバッジを利用した図である。

図 3 4 は、携帯端末の間で送受信の行われる様子を示す図である。

15 発明を実施するための最良の形態

<概略構成>

以下、本発明の実施形態を図面を参照して説明する。

図 1 は、本発明の一実施形態による情報保護システムの概要を示すブロック図である。この情報保護システムは、第 1 の I C アセンブリ 3 0 と第 2 の
20 I C アセンブリ 4 0 とで構成される。第 1 の I C アセンブリは、中央処理装置（C P U）3 1 と、無線通信インタフェース部 3 2 と、照合用データ記録部 3 3 と、トリガ信号受信部 3 4 と、被保護情報記録部 3 5 とを備えている。同様に、第 2 の I C アセンブリ 4 0 は、C P U 4 1 と、無線通信インタフェース部 4 2 と、照合用データ記録部 4 3 とを備えている。また、第 1 および
25 第 2 の I C アセンブリ 3 0 および 4 0 は、各アセンブリで必要なアプリケーションプログラムや制御プログラム、オペレーティングシステム（O S）、デバイスドライバなどが格納された図示しない読取専用メモリ（R O M）やランダムアクセスメモリ（R A M）を含む。

第 1 の I C アセンブリ 3 0 および第 2 の I C アセンブリ 4 0 は、無線を利

用して互いにデータの送受信が可能なように構成されている。この場合、本願明細書において使用する「無線通信」という用語は、金属端子による電氣的な接触を使用せずに行う通信全般を意味し、一例として、非接触自動識別システム（RFID:Radio Frequency Identifcation）で用いられている

5 電磁結合方式、電磁誘導方式、マイクロ波方式、光方式の無線通信があげられる。また、米国特許第6,211,799号（特開平11-225119号）に開示されているような人体を介して電力と情報を伝送するための方法による通信も本願明細書における「無線通信」に包含されるものとする。

CPU31は、第1のICアセンブリ30の各構成要素を制御し、CPU

10 41は第2のICアセンブリ40の各構成要素を制御する。無線通信インタフェース部32および42は、それぞれが送信機能と受信機能の両方を有する。この無線通信インタフェース部32および42は、たとえばRFID技術において用いられているようなアンテナやコイルなどを有し、互いにデータの送受信を行うものである。

15 RFIDにはさまざまな変調方式や周波数、通信プロトコルを利用したものがあるが、本発明は特定の方式に限定されるものではなく、どのような方式を利用してもよい。ICアセンブリに設けられる無線通信インタフェース部の数にも特に制限はなく、必要に応じて異なる変調方式で機能する無線通信インタフェース部を複数設けるようにしてもよい。なお、汎用性の観点から

20 見ると、非接触型ICカードの分野で標準規格化が進められている仕様に準拠するなどの方式を採用すると好ましい。日本においては、次世代ICカードシステム研究会（the Next Generation IC Card System Study Group）やICカードシステム利用促進協議会（Japan IC Card System Application Council）が標準化活動を行っている。また、すでに確立されている国際規格として、ISO/IEC10536、ISO/IEC14443、ISO/IEC15693がある。このような規格に準拠した無線通信インタフェース部32および42とすることで、より一層汎用的かつ

25 実用性の高い情報保護システムを構築できる可能性がある。

照合用データ記録部 3 3 および 4 3 には、第 1 および第 2 の I C アセンブリの照合を行うためのデータが記録されている。この照合用データが所定の条件を満たした場合に限り、被保護情報記録部 3 5 へのアクセス、例えば被保護情報記録部 3 5 に格納されたデータやプログラムへのアクセスが許可
5 される。照合用データとは、I C アセンブリの所有者を一意に特定するためのデータであり、その内容は特に限定されるものではない。たとえば C P U の固有記号や製品番号、クレジットカード番号、これらの一意なデータを複数組み合わせたものや、さらにこれを暗号化したものなどを照合用データとして利用することができる。被保護情報とは、個人情報や金銭的価値のある
10 情報など、I C アセンブリの所有者が第三者による閲覧や使用を制限し、保護することを希望する情報またはデータであれば、どのような情報またはデータであってもよい。一例として、クレジットカード、キャッシュカード、プリペイドカード、各種会員権、診察券、健康保険証、身分証明書、公共施設のチケットなど従来のカード類に記録されたデータの他、電子マネーや電
15 子取引情報、私的な住所録やドキュメント、画像データなど、さまざまなものが考えられる。

図 2 に、I C アセンブリ 3 0 へのアクセス要求に対しての I C アセンブリ 3 0 の C P U 3 1 における認証処理を表すフローチャートを示す。

無線通信インタフェース部 3 2 は、トリガ信号受信部 3 4 と接続され、後
20 述するトリガ信号を受信する。C P U 3 1 は、トリガ信号受信部 3 4 でトリガ信号が受信されないときは、I C アセンブリ 3 0 に対するアクセス要求は無しと判定し、トリガ信号が受信された場合はアクセス要求有りと判定する（S 1 1）。トリガ信号が検出された場合、C P U 3 0 は、無線通信インターフェース 3 2 を通じて、当該トリガ信号に応答して第 2 の I C アセンブリ
25 4 0 に対して照合用データの送信を要求する要求信号を送信する（S 1 2）。第 2 の I C アセンブリ 4 0 は、この要求信号に応答して、自己の照合用データ記録部 4 3 に格納された照合用データを第 1 の I C アセンブリに送信する。C P U 3 1 は、無線通信インターフェース 3 2 を通じて照合用データが受信されたか否かを判定し（S 1 3）、受信さない場合はアクセスを拒否す

る（S 1 4）。照合用データが受信された場合、CPU 3 1 は、第 2 の IC アセンブリ 4 0 から受信した照合用データと IC アセンブリ 3 0 の照合用データ記録部 3 3 に格納された照合用データとの比較処理を開始させる（S 1 5）。この例では、この比較は、比較部 3 6 によって行われる。

- 5 比較部 3 6 における比較の結果、所定の条件が満たされたか否かを判定する。この例では、IC アセンブリ 4 0 から受信したデータと IC 照合用データとが一致するか否かを判定し（S 1 6）、一致した場合には、CPU 3 1 は、アクセスを許可し（S 1 7）、被保護情報記録部から必要な情報を抽出する。一方、所定の条件が満たされなかった場合は、CPU 3 1 は被保護情報記録部 3 5 に格納されたデータへのアクセスを禁止する（S 1 4）。

- 照合用データ記録部 3 3、4 3、被保護情報記録部 3 5 などの記録部は、たとえば IC チップなどの記録素子で実現される。なお、図 1 に示す例では照合用データの比較を第 1 の IC アセンブリ 3 0 において行ったが、第 2 の IC チップアセンブリ 4 0 側で比較を行うことも可能である。この場合、比較を行なった後に第 2 の IC アセンブリ 4 0 から第 1 の IC アセンブリ 3 0 に比較の結果を無線通信にて通知し、CPU 3 1 は当該比較の結果に応じて被保護情報記録部 3 5 へのアクセスを許可するか否かを判断する。あるいは、第 1 の IC アセンブリ 3 0 と第 2 の IC アセンブリ 4 0 の両方に比較部を設け、異なる照合用データをやり取りして双方で所定の条件が満たされた場合
- 15 合にのみ被保護情報記録部 3 5 へのアクセスが可能なような形態にしてもよい。特に後者のような二重照合形態にすることで、被保護情報記録部 3 5 に格納されたデータを一層確実に保護することができる。

- 上述した第 1 および第 2 の IC アセンブリは、周知の半導体製造技術を用いて製造可能なものであるが、本発明は半導体による集積回路に限定されるものではない。たとえば、光電子集積回路（OEIC）やバイオ系チップを用いて第 1 および／または第 2 の IC アセンブリを製造してもよい。このようにして製造した IC アセンブリは、小型チップとしてさまざまな物体に埋め込むことが可能なものである。以下、本発明の目的において、IC アセンブリを装飾品や衣類など所有者の身近におくことが可能な物体に埋め込ん
- 25

だものを「R バッジ」と総称する。また、個人情報や金銭的価値の付帯する情報を携帯端末に統合したものを「多目的携帯端末」と総称する。

次に、図 3 を参照すると、第 1 の I C アセンブリを多目的携帯端末 3 0 0 の形で実現し、第 2 の I C アセンブリを R バッジ 4 0 0 の形で実現した例が示されている。多目的携帯端末 3 0 0 はスイッチ 3 0 1 を備え、端末の所有者がスイッチ 3 0 1 を押すことでトリガ信号が生成される。トリガ信号受信部 3 4 (図 1) は、トリガ信号を受信すると、無線通信インタフェース部 3 3 に対して第 2 の I C アセンブリとの間での通信を開始するよう指示する。これ以降の照合動作については図 1 を参照して説明したとおりである。このようにすることで、多目的携帯端末と R バッジとの間で照合用データを照合し、照合の結果が所定の条件を満たした場合に限って多目的携帯端末を使用可能とすることができる。

図 4 は、自動改札機に非接触型 I C カード用のリーダライタ 5 0 を設け、このリーダライタから送信される信号 (プリチャージ信号) をトリガ信号として利用した例を示している。この場合、リーダライタから発信される信号は、周知の R F I D システムにおいて利用されている信号と同様のものである。利用者が多目的携帯端末 3 0 0 を自動改札機に近づけると、リーダライタ 5 0 から発信されるプリチャージ信号に応答して多目的携帯端末 3 0 0 が R バッジ 4 0 0 との通信を開始する。これ以降の照合動作については図 1 を参照して説明したとおりである。利用者は多目的携帯端末を自動改札機に近づけるだけで、改札を通ることができるという利点がある。自動改札機に限らず、金融機関の A T M や公衆電話など、決済や金銭の移動を伴う行為に関わる多くの設備に同様の方式を応用することが可能である。

また、照合結果が所定の条件を満たした後所定時間が経過する前に被保護情報へのアクセスがなされた場合はそれを許可し、この所定時間が経過した後の場合はアクセスを禁止するようにしてもよい。この場合、例えば、I C アセンブリ 3 0 または 4 0 のいずれか一方または両方にタイマを設けることで、上述のような所定時間が経過したか否かを検出することが可能となる。このような方法をとることで、I C アセンブリ 3 0 と 4 0 との間の距離が通

通信可能距離よりも長い場合であっても本発明を実現することが可能である。

以下、多目的携帯端末 300 に乗車券を統合して自動改札機を通過する場合を例に説明する。なお、この例では、多目的携帯端末 300 (IC アセンブリ 30) と IC アセンブリ 40 との間の通信可能距離が 10 cm であるものとする。通常の自動改札機においては、多目的端末 300 を手で保持した状態で自動改札機のリーダライタ 50 に近づけて認証を行う。IC アセンブリ 40 が例えば指輪に実装されているのであれば、多目的端末 300 内の IC アセンブリと指輪との間隔は 10 cm よりより短いので、問題なく認証を行うことができる。しかし、IC アセンブリ 40 が帽子あるいはイヤリングに実装されている場合、IC アセンブリ 30 と IC アセンブリ 40 との間の距離は、通常は 10 cm よりも長くなり、認証を行うことができなくなる。

このような場合、多目的携帯端末 300 を帽子あるいはイヤリングに近づけて IC アセンブリ 30 と IC アセンブリ 40 との距離を 10 cm 以下としたうえで、IC アセンブリ 40 と IC アセンブリ 30 との間での認証を行わせる。この動作は、例えば図 3 の例では、多目的携帯端末 300 を帽子またはイヤリングの近傍に持っていった状態で、多目的携帯端末 300 のスイッチ 301 を押してトリガ信号を発信させることにより認証を行う。

また、図 4 の例では、リーダライタ 50 から発信されるプリチャージ信号に応答可能な範囲内に多目的携帯端末 300 がある状態で、多目的端末 300 を耳元に近づけて帽子又はイヤリングに実装された IC アセンブリ 40 との距離を 10 cm 以下とすることで、認証を行い、携帯端末 300 に記録された乗車券のデータを利用可能とすることができる。このように、タイマを設けて一定のタイムラグを許容することで、IC アセンブリ 30 と IC アセンブリ 40 とを実際に使用するときの距離が比較的長い場合であっても、通信可能距離の短い通信方式を採用することが可能になる。

また、携帯端末に保存された情報を、専用のサーバにバックアップしたり、仕様内容のログファイルを保存することにより、それらの情報を必要に応じてダウンロードし、紛失前の状態に復帰できるようにしてもよい。

更に、所有者は IC カードをそのまま使うか IC カード機能を内蔵した携

帯端末として使うかを選択することができる。さらに、ＩＣアセンブリ３０に周知のＧＰＳ機能を内蔵させることで、ＩＣアセンブリ３０を紛失したようなときにも被保護情報記録部３５に記録されたデータに対する保護性を一層高めることができる。

- 5 次に、本発明を端末等に適用した実施の形態を以下の“第１の実施の形態”～“第７の実施の形態”を例にとって詳細に説明する。

第１の実施の形態における携帯端末１０は、図５に示すように、電波認識方式でデータの送受信を行う送受信部２０と、ＲＡＭやＲＯＭなどからなるメモリ３０と、ＣＰＵ（中央制御処理装置）などからなる制御部４０から概
10 略構成される。

電波認識方式とは、ＲＦＩＤなどに代表される送受信方式で、電氣的な接続を行わずにデータが送受信されるもので、電磁結合・電磁誘導・マイクロ波・光などを利用したものである。

- この携帯端末１０は、携帯電話、ＰＨＳ、ＰＤＡ（携帯情報端末）、ノートパソコンなどの端末である。電波認識方式で送受信するインターフェースを、以下、ＲＦＩＤインターフェースと呼ぶ。
15

制御部４０は送受信部２０やメモリ３０に接続して、送受信部２０やメモリ３０を制御する。

- 送受信部２０には、発信部（或いは、送信部）と受信部を兼ね備えたもので、アンテナ２２を介してＲＦＩＤインターフェースを備えた記録素子など
20 からデータを読み取る機能や、記録素子などにデータを書き込む機能、或いは、ＲＦＩＤインターフェースを備えた読取装置にデータを発信する機能などを備える。

- 記録素子とは、ＩＣチップなどである。以下、記録素子をＩＣチップとして説明する。
25

また、送受信部２０は、通信制御用ＩＣなどからなる通信制御用部２１とアンテナ２２などから構成される。ここでは、通信制御用部２１を通信制御用ＩＣとして以下説明する。

さらに、送受信部２０の通信制御用ＩＣ２１は制御部４０と接続され、制

御部 40 からデータを読み込むためのコマンドを受け取りアンテナを介してデータを送受信するものである。

メモリ 30 は制御部 40 と接続され、データを格納する部分や、OS（オペレーティングシステム）や通信制御用 IC 21 を制御するデバイスドライバなどの制御プログラム、さらに、アプリケーションプログラムなどを備えている。

RFID インターフェースには、さまざまな変調方式・周波数・通信プロトコル等がある。そこで、図 6 に示すように、それぞれに対応した、通信制御用 IC 21 やアンテナを用意し、さらに、通信制御用 IC 21 を制御するデバイスドライバなどの制御プログラムを携帯端末 10 に複数用意して必要に応じて選択可能なように構成することもできる。

また、標準化の観点からすると、密着型として ISO/IEC 10536、近接型として ISO/IEC 14443、近傍型として ISO/IEC 15693 の RFID インターフェースを備えることが好ましい。また、キャリア周波数としては、125 kHz ~ 400 kHz、4.9152 MHz、13.56 MHz、2.45 GHz のものが考えられる。

また、RFID インターフェースには、例えば、一方を体に装着し一方を手につくと人体を通して送受信することが可能なものもある。このように、伝導性のあるものを媒介にして送受信をおこなう機能を持たせることもできる。

さらに、上述したものに限らず、必要に応じて他の方式の RFID インターフェースの組み込みが可能である。

また、携帯端末 10 には、図 7 のブロック図に示すように、各 RFID インターフェースに対応した送受信部 20 と、この各 RFID インターフェースを利用するためのデバイスドライバ（制御プログラム）31 とを複数用意し、OS（オペレーティングシステム）などからなるシステム管理部 32 上でさまざまなアプリケーションプログラム 33 を動作させることができ多種多様な機能を持たせることが可能である。さらに、必要に応じて、アプリケーションプログラム 33 で利用するデータを格納するデータ格納部 34

を持つ。

さらに、このアプリケーションプログラム 33 やデバイスドライバ 31 は、インターネットなどのネットワークからダウンロードして、新たな機能の追加や、更新することが可能である。

- 5 また、ICカードにも、前述したRFIDインターフェースと同様の構成を備えている。図8に示すように、ICカード50にはICチップ51がアンテナ22と接続されている。

- 10 記録素子であるICチップ51には、通信制御用IC21とCPUなどからなる制御部40とメモリ30を備え、アンテナ22を介してデータの送受信を行う。メモリ30は制御部40と接続され、データをメモリに格納する部分や、通信制御用IC21を制御するソフトウェアを備えている。さらに、OSを備えるようにしても良い。

あるいは、通信制御する部分を集積回路とすることも可能である。

- 15 また、図示しないが、あらゆる装置に前述したRFIDインターフェースの送受信部20を組み込むことができ、RFIDインターフェースでデータの送受信を行う機能を持たせることが可能である。

次に、送受信部20の送受信を行う仕組みについて、電磁誘導を使って送受信する例について具体的に説明する。

- 20 ここでは、図9に示すように、送受信部20を受信部20'と発信部（送信部）20''とに分けて説明する。

まず、受信部20'では、通信制御用IC21には、制御部40から読み取りのコマンドを受けてデータの読み取りを開始する読み取り制御部211と、受信したデータを制御部40'に渡すデータ受信部212とを備える。

- 25 読み取り制御部211は、制御部40'から読み取りのコマンドを受け取ると発信要求としてパワーパルスを発生してアンテナ22'から送出する機能を備える。また、データ受信部212は、発信部20''からのデータをアンテナ22'で受信するとデータをデコードして制御部40'に渡す機能を備える。

発信部20''には、電磁誘導によるキャパシティを蓄える蓄電部213と、

データを送信するデータ送信部 214 と備える。

蓄電部 213 は、アンテナ 22'' で受信部 20' から発信要求としてパワーパルスを受け取ると蓄電する機能を備える。また、データ送信部 214 では、蓄電部 213 に蓄えられたエネルギーを電源としてアンテナ 22'' から
5 データを発信する機能を備える。

また、発信部 20'' に、電源が接続される構成になっている場合には、パワーパルスを受信信号としてのみ利用し、蓄電部 213 を備えない構成とすることも可能である。

送受信部 20 は、受信部 20' と発信部（送信部） 20'' の双方の機能を
10 兼ね備えるものである。

次に、本実施の形態の動作をフローチャートに従って説明する。

ここでは、RFID インターフェースを備えた IC カードや装置からデータを受信する場合を例に、携帯端末 10 の受信の動作を図 10 のフローチャートを用いて説明する。

15 まず、RFID インターフェースを備えた IC カードや装置などの近くに携帯端末 10 を持っていく。RFID インターフェースを備えた IC カードや装置と携帯端末 10 とが送受信可能な距離は、密着型か、近接型か、近傍型かによって違う。密着型か、近接型か、近傍型かは目的により使い分けられ、アプリケーションプログラムで選択されたデバイスドライバを用いて送
20 受信を行う（S100）。アプリケーションプログラムからデバイスドライバに読み取りのシステムコールを呼び出すと、デバイスドライバから通信制御用 IC 21 に読み取りのコマンドが送られる（S101）。通信制御用 IC 21 は、読み取りのコマンドを受け取ると読み取り制御部 211 を介してアンテナ 22（22'）より発信要求としてパワーパルスを発生する。

25 IC カードや装置は、発信要求としてパワーパルスを受け取り、電磁誘導で発生した電流は蓄電部 213 に蓄える（S200）。蓄電部 213 に蓄えられた電力を使用してデータをアンテナ 22'' から発信する（S201）。

携帯端末 10 は、アンテナ 22（22'）を介してデータを受信し（S103）、データ受信部 212 を介してデコードされたデータは、デバイスド

ライバからアプリケーションプログラムに渡される。

次に、R F I D インターフェースを備えた I C カードや装置などにデータを発信する場合を例に、携帯端末 1 0 の発信の動作を図 1 1 のフローチャートを用いて説明する。

- 5 I C カードや装置では通信制御用 I C 2 1 に読み取りのコマンドを送る (S 2 1 0) と、I C カードや装置の通信制御用 I C 2 1 は、読み取りのコマンドを受け取ると読み取り制御部 2 1 1 を介してアンテナ 2 2 (2 2') より発信要求としてパワーパルスを発生する (S 2 1 1)。

- 10 携帯端末 1 0 は、発信要求としてパワーパルスを受け取ると (S 1 1 0)、それを C P U の割り込み信号として利用し、データをアンテナ 2 2 (2 2'') から発信する (S 1 1 1)。あるいは、電磁誘導で発生した電流を蓄電部 2 1 3 に蓄え、蓄電部 2 1 3 に蓄えられた電力を利用してデータを発信しても良い。

- 15 I C カードや装置は、アンテナ 2 2 (2 2') を介してデータを受信する (S 2 1 2)。

ここでは、携帯端末 1 0 には送受信部に受信部の機能と発信部 (送信部) の機能を備えたものについて説明したが、受信部の機能か発信部 (送信部) の機能かいずれかを一方のみを備えたものでも良い。

- 20 また、ここでは電磁誘導による例について説明したが、データを受信する側から発信要求としてポーリングしてデータを受信するようにしても良い。

さらに、送受信部 2 0 は携帯端末 1 0 に脱着可能なユニットとし (例えば、カード型ユニットなど)、さまざまな R F I D インターフェースを装着することが可能である。

- 25 あるいは、記録素子には半導体以外のものを利用して I C チップと同様の機能をもつもので構成するようにしても良い。

以上、説明したように R F I D インターフェースを備えた携帯端末 1 0 を利用して、I C カード 5 0 とデータの送受信を行うことができる。さらに、R F I D インターフェースを備えた装置ともデータの送受信が行うことができる。

また、携帯端末 10 で IC カード 50 や装置に記憶されている固有のデータを読み込むと、アプリケーションを起動することも可能である。例えば、IC カード 50 の情報を読み込むとインターネットに接続する。あるいは、RFID インターフェースを組み込んだ装置から情報を読み込むと、説明書
5 などを表示することもできる。

第 2 の実施の形態では、携帯端末 10 に（IC カードで行われている）定期券・乗車券・クレジットカード・鍵などの機能を内蔵させる個別情報システムについて説明する。ここでは、クレジットカードなどカード機能を携帯
10 端末 10 に内蔵させる場合を例に説明する。前述の実施の形態と同一のものには同一符号を伏して詳細な説明を省略する。

他の実施の形態における個別情報

システム 11 は、図 12 に示すように、携帯端末 10 と RFID インターフェースの送受信部 20'（受信部）を組み込んだ受信装置 60 とで概略構
15 成される。

受信装置 60 は、送受信部 20' と制御部 40' が設けられ、携帯端末 10 から個別情報を読み取る機能を備えている。この受信装置 60 に携帯端末 10 を近づけて個別情報を読み取るようにするため、送受信部 20' には、近接型を使用することが好ましい。

20 携帯端末 10 は、図 13 に示すように、メモリ 30 上のデータ格納部 34 に個別情報 340 を記憶する。ここでは、個別情報 340 としてカード情報を記憶している例について説明する。

個別情報 340 には、複数のカード情報（例えば、図 13 の A、B、C）を記憶することも可能でその中から利用するカードを選択する機能を備える。さらに、カードに応じたアプリケーションプログラム 33 を複数用意し、
25 各カードに応じた機能を持たせることが可能である。

以下、個別情報 340 をカード情報と置き換えて説明する。

次に、本実施の形態の動作を図 14 のフローチャートに従って説明する。

携帯端末 10 で、利用するカードを選択して（S120）、携帯端末 10

を受信装置 60 に近づける。受信装置 60 では、例えば、受信装置 60 に設けられている読み取りスイッチの押下によって、カード情報 340 の読み取り指示を受け取ると、読み取りコマンドを送受信部 20 に送る (S 220)。そこで、送受信部 20 から指定されているカードのカード情報 340 (個別
5 情報) の発信要求 (パワープルスなど) を携帯端末 10 に発信する (S 221)。

携帯端末 10 では、カード情報 340 の発信要求を受け取ると選択されているカード情報 340 を発信する (S 122)。受信装置 60 では、受信したカード情報 340 が、要求したカード情報であれば処理を続行するが (S
10 224)、要求したカード情報でない場合はエラー終了する (S 225)。

本実施の形態では、携帯端末 10 にカード機能を持たせる場合について説明したが、定期券や乗車券の機能を持たせることも可能である。この場合には、受信装置 60 の送受信部 20 には、多少離れた位置から読み取り可能なように近接型を利用することが好ましい。

15 また、携帯端末 10 に鍵の機能を持たせることも可能である。この場合には、受信装置 60 の送受信部 20 には、やや離れた位置から読み取り可能なように近傍型または近接型を利用することが好ましい。

また、電子マネー・クレジットカード・会員権・診察券・健康保健所・身分証明書・アミューズメント施設のチケット類の機能を持たせることも可能
20 である。

さらに、個別情報 340 は、携帯端末 10 の固体それぞれを識別する識別情報を利用することもできる。

さらにまた、携帯端末 10 を買い換えるなど置き換えをする場合には、携帯端末 10 に記録されている電子マネー・クレジットカード・会員権などを
25 管理する管理会社にインターネットなどを介して置き換えを通知する。そこで、古い携帯端末 10 では利用できないようにし、新しい携帯端末 10 にその情報をダウンロードして利用するようにすることも可能である。

以上、説明したように、携帯端末 10 に、複数の機能を兼ね備えるようにすることが可能である。

第3の実施の形態では、識別情報を記憶するICチップを利用して携帯端末10の利用者を識別する利用者識別システムについて説明する。前述の実施の形態と同一のものには同一符号を伏して詳細な説明を省略する。

5 いつも身に付けているものや身近におくものにICチップを埋め込んだものを総称して、以下、レッドバッジと呼ぶ。

第3の実施の形態における利用者識別システム12は、図15に示すように、携帯端末10と識別情報を記憶する携帯記録素子とで概略構成される。以下、携帯記録素子としてICチップ51とアンテナ22を組み込んだレッドバッジ70を例に説明する。

10 ここで、ICチップ51を内蔵したレッドバッジ70の例について説明する。レッドバッジ70は、第1のタイプとして、図16に示すように、指輪・イヤリング等の本体をアンテナ22として本来の目的と共用し、それにICチップ51が備えられるタイプがある。

第2のタイプとして、図17に示すように、ネクタイピン等の本体61に
15 ICチップ51とアンテナ22が内蔵される。或いは、図18に示すように、カフスボタン・バッジ・ブローチ・ペンダント・コンタクトレンズ等の本体62にICチップ51とアンテナ22が内蔵されたものなど身につけるものに内蔵されるタイプがある。

他にも、財布・パスケース等の本体にICチップ51とアンテナ22が内
20 蔵される。筆記用具・ライター等の本体にICチップ51とアンテナ22が内蔵されたものなど身近におくものに内蔵されるタイプがある。

以上、例に挙げたものだけでなく、様々なものにICチップ51を内蔵することができアンテナ22の形状も多様である。

また、図19に示すように、レッドバッジ70に内蔵されたICチップ5
25 1には、識別情報をメモリ30の識別情報記憶部35に格納する。識別情報記憶部35はROMなど書換不可能な記録素子で構成されることが望ましい。また、識別情報350は一意に識別できるように割り振ったものである。識別情報350はレッドバッジ70の製造時に、一意となるように書き込むようにしても良い。

また、携帯端末 10 の近傍に複数の第 3 者のレッドバッジ 70 が存在する場合を考慮すると、携帯端末 10 とレッドバッジ 70 は、近接していないと識別情報 350 が読み取れないようにするほうが望ましい。近接とは、使用している携帯端末 10 と、使用者が衣類につけるなど身につけた状態のレッドバッジ 70 とが送受信可能な程度である。

以上の条件を考慮に入れると、レッドバッジ 70 には、近接型または密着型の IC チップを使用することが好ましい。さらに、レッドバッジ 70 と携帯端末 10 との送受信可能な範囲は数十センチメートル以下であることが望まれる。

次に、本実施の形態の動作をフローチャートに従って説明する。

識別情報 350 を登録する動作について、図 20 のフローチャートを用いて説明する。以下、フローチャートではレッドバッジ 70 を R バッジとする。

まず、携帯端末 10 にレッドバッジ 70 の識別情報 350 を登録するための登録モードにする (S 130)。この登録モードにする際には、暗証番号やバイオメトリックス (アイリス、声紋、指紋など) を入力しないと登録モードにならないようにし、第 3 者では登録できないようにする。登録モードになると、読み取り開始のコマンドを制御部 40 から通信制御用 IC 21 に送信するとアンテナ 22 から発信要求 (パワーパルスなど) を発信してレッドバッジ 70 の読み取りを開始する (S 131)。

ここで、携帯端末 10 のタイマーに所定の時間 t を設定する (S 132)。そこで、時間 t が経過するまで (S 134)、レッドバッジ 70 から識別情報 350 を受信したか繰り返しチェックする (S 133)。

時間 t が経過しても、レッドバッジ 70 から識別情報 350 の受信が完了しない場合は、携帯端末 10 の画面上にエラーメッセージを表示する (S 135)。或いは、受信した識別情報がすでに登録済みの識別情報の場合には、携帯端末 10 の画面上にエラーメッセージを表示する (S 135)。

受信した識別情報 350 が登録済みの識別情報でない場合は、識別情報 350 を携帯端末 10 のメモリ 30 に格納して登録する。

携帯端末 10 を使用する際に、近傍にあるレッドバッジ 70 の識別情報 3

50を確認する動作について、図21のフローチャートを用いて説明する。
図21のフローチャートで説明するデフォルトモード1は、操作を開始しレ
ッドバッジ70の識別情報350が読み込まれたときに解除されるもので、
通常操作を行っていない状態とする。また、デフォルトモード2は、いたず
5 らされている可能性があるため、解除には暗証番号やバイオメトリックスな
どを入力して本人である確認をする必要がある状態として以下説明する。

まず、携帯端末10を使用する者がキー入力などの携帯端末10を使用す
るための初動作を行った時点で、制御部40のCPUには割り込みが発生す
る(S150)。割り込みが発生すると、読み取り開始のコマンドを制御部
10 40から通信制御用IC21に送られる。通信制御用IC21は、読み取り
開始のコマンドを受け取るとアンテナ22から発信要求を発信して読み取
りを開始する。

ここで、制御部40はタイマーに所定の時間t1を設定し(S151)、
レッドバッジ70から発信した識別情報350を受信したかチェックする
15 (S152)。時間t1が経過するまで識別情報350の受信したかを繰り
返しチェックする(S153)。時間t1が経過しても、レッドバッジ7
0から識別情報350の受信が完了しない場合は、デフォルトモード1を設
定する(S162)。

識別情報350の受信が完了した場合は、受信した識別情報がメモリ30
20 に予め登録されている識別情報と比較し、該当するものがある場合には、登
録済みのレッドバッジ70が近くにあるので携帯端末10の利用が可能で
ある(S154)。該当するものがない場合には、登録済みのレッドバッジ
70ではない。そこで、登録されていない識別情報の受信回数が指定の回数よ
り少ない場合は、デフォルトモード1を設定する(S162)が、登録され
25 てない識別情報の受信回数が指定の回数より多い場合は、デフォルトモード
2を設定する(S163)。

登録されている識別情報を受信した場合には(S154)、さらに、所定
の時間t2をタイマーに設定する(S156)。時間t2が経過するまでに
(S158)、通話・メール受信・インターネットのアクセスなどの処理を

開始しなかった場合は（S 2 0 7）、デフォルトモード 1 を設定する（S 1 6 2）。

時間 t_2 が経過するまでに（S 1 5 8）、開始した通話・メール受信・インターネットのアクセスなどの処理が終了した場合は（S 1 5 7）、所定の
5 時間 t_3 をタイマーに設定する（S 1 5 9）。時間 t_3 が経過するまでに（S 1 6 1）、通話・メール受信・インターネットのアクセスなどの次の処理を開始した場合には（S 1 6 0）、レッドバッジ 7 0 の読み込みをすることはなく、引き続き作業を行うことができる。一つの作業が終了するたびに t_3 が起動され（S 1 5 9）、 t_3 以内に次の作業が開始されないときは（S 1
10 6 1）、デフォルトモード 1 になる（S 1 6 2）。

図 2 1 のフローチャートでは、携帯端末 1 0 を利用する初動作に伴って発生した割り込み処理で、近傍にあるレッドバッジ 7 0 の識別情報を確認する処理について説明したが、携帯端末 1 0 を使用する際に、この割り込みの処理と同時に使用者の操作に応じた処理が平行して実行される。

15 また、デフォルトモード 2 の場合には、機能を停止し予め設定した動作をする。例えば、着信音を最大にして警告を発する。或いは、ダイヤルロックにすることも可能である。

デフォルトモードは各携帯端末 1 0 の出荷時に設定されているが、購入後それぞれに応じた動作が使用者が任意に設定することができる。また、セキュリティレベルに応じて、携帯端末 1 0 を利用する前には暗証番号を必ず入力しなければ使用できないようにするなど、使用者で変更可能である。
20

また、識別情報 3 5 0 の受信は、操作時の割り込み処理を使った例について説明したが、携帯端末 1 0 からポーリングをしてレッドバッジ 7 0 から識別情報 3 5 0 を受信し、定期的にレッドバッジ 3 の有り無しを確認すること
25 も可能である。

さらに、図 2 2 に示す使用者識別システム 1 2' のように、第 2 の実施の形態で説明したように、携帯端末 1 0 に定期券・乗車券・クレジットカード・鍵などの機能を内蔵させ、その機能を受信装置 6 0 で受け取る場合に、まず、携帯端末 1 0 の使用者が正当な使用者かをレッドバッジ 7 0 で確認を取る

ようにすることも可能である。

以上、説明したようにレッドバッジに組み込んだ携帯記録素子の識別情報を確認して携帯端末10の使用を可能にすることができ、正当な使用者にのみ使用を許可することができる。

- 5 第4の実施の形態では、携帯端末10でICチップなどの記録素子にデータを書き込む機能に付いて説明する。前述の実施の形態と同一のものには同一符号を付して詳細な説明を省略する。

第4の実施の形態における携帯記録素子書込システム13は、図23に示すように、携帯端末10と記録素子51とアンテナ22を組み込んだICカード50とで概略構成される。ここでは、記録素子51とアンテナ22を組み込んだICカード50にデータを書き込む場合を例に説明する。

記録素子51は、識別情報350を記録しているものである。

次に、本実施の形態の動作を図24のフローチャートに従って説明する。

- まず、携帯端末10で書き込みモードの選択をした時点で、制御部40のCPUには割り込みが発生する(S170)。割り込みが発生すると、読み取り開始のコマンドを制御部40から通信制御用IC21に送られる。通信制御用IC21では読み取り開始のコマンドを受け取るとアンテナ22から読み取り要求(パワーパルスなど)を発信してICカード50に登録されている識別情報350の読み取りを開始する。

- 20 ここで、携帯端末10の制御部40はタイマーに所定の時間t1を設定し(S171)、ICカード50から発信した識別情報350を受信したかチェックする(S172)。時間t1が経過するまで識別情報350の受信を繰り返しチェックを行い(S173)、時間t1が経過しても、ICカード50から識別情報350の受信が完了しない場合は、カードの認識不能の表示を行う(S180)。

識別情報350の受信が完了した場合は、受信した識別情報がメモリ30に予め登録されている識別情報と比較して、該当するものがある場合には(S174)、登録済みのICカード50であるとする。該当するものがない場合には(S174)、登録済みのICカード50ではないので書込不可

の表示をする（S 1 8 1）。

登録済みの I C カード 5 0 の場合は、まず、書込カウンター C を設定する（S 1 7 5）。書込処理（S 1 7 6）を行い正常に書込処理が終了しない場合は（S 1 7 7）、書込カウンター C が 0 になるまで（S 1 7 8）、再度書込
5 処理（S 1 7 6）をする。書込カウンター C が 0 になっても書き込みができない場合は書込不良を表示する（S 1 8 2）。

正常に書き込みが終了すると書込終了を表示する（S 1 7 9）。

以上、説明したように、R F I D インターフェースを備えた携帯端末 1 0
10 では、受信したデジタルチケットなどのデジタル情報を I C カード 5 0 に書き込むことが可能である。また、携帯端末 1 0 を利用してインターネットなどの銀行からキャッシングして I C カード 5 0 に書き込むことも可能である。

さらに、図 2 5 に示す携帯記録素子書込システム 1 3' のように、I C カード 5 0 に書き込みを行う際、第 3 の実施の形態で説明したように携帯端末
15 1 0 の使用者が正当な使用者かをレッドバッジ 7 0 で確認を取るようにすることも可能である。

これにより、正当な携帯端末 1 0 の利用者のみ I C カード 5 0 に書き込みが行える。

第 5 の実施の形態では、インターネットなどの回線を利用して携帯端末 1
20 0 や I C カード 5 0 の利用状況を管理する第 1 の利用管理システムについて説明する。前述の実施の形態と同一のものには同一符号を伏して詳細な説明を省略する。

第 5 の実施の形態における利用管理システム 1 4 は、図 2 6 に示すように、
25 携帯端末 1 0 や I C カード 5 0 などの記録素子と R F I D インターフェースの送受信部を組み込んだ装置 9 0 と管理サーバ 1 0 0 とが通信回線 1 1 0 を介して接続される。さらに、通信回線 1 1 0 には、銀行の端末やネットバンクなどの金融機関 1 2 0 が接続される構成になっても良い。

この携帯端末 1 0 や I C カード 5 0 などの記録素子には、各個体が一意に識別できる識別情報 3 5 0 が書換不可能に記録されている。また、携帯端末

10 には、RFIDインターフェースの送受信部20を備え、識別情報350を発信する機能を備える。さらに、携帯端末10には、通信回線送信部25を備え、通信回線を介してインターネットなどに接続する機能を備えている。

5 ここでは、装置90は、自動販売機にRFIDインターフェースの送受信部を組み込んだものを例に説明する。装置90より、RFIDインターフェースを備える携帯端末10やICカード50などと送受信することが可能で、代金を携帯端末10やICカード50に記録されているプリペイドカードやキャッシュカードなどから代金を受領する機能を備えている。

10 また、装置90には、管理サーバ100と通信回線110を介して送受信を行うサーバ接続部80を備える。さらに、装置90には、装置毎に割り振られる装置番号91を記録している。

管理サーバ100は、携帯端末10やICカード50の識別情報350とその利用情報とをともに通信回線110を介して受信し、利用内容を表す利用情報を管理する管理部を備える。

15 通信回線110は、専用回線やインターネットなどである。情報管理の信頼性の観点から、セキュリティの確保されているものが好ましい。

次に、本実施の形態の動作を携帯端末10を例に、図27のフローチャートと図28の携帯端末10の画面の遷移図に従って説明する。

20 まず、携帯端末10では、図28の画面の遷移図に示すように、メニューからプリペイドカードのモード1000～商品購入モード1001～自動販売機モード1002を選択する(S300)。ここで、識別情報350を携帯端末10のRFIDインターフェースから自動販売機90に発信すると、携帯端末10には、個人認証中の画面1003が表示される(S301)。

25 以下、自動販売機90と携帯端末10とは、RFIDインターフェースで送受信されるものとする。

自動販売機90では、識別情報350を受け取ると、携帯端末10の識別情報350と自動販売機90の装置番号91とを管理サーバ100にサーバ接続部80から送信して、残高確認及びブラックリストとの照合を行う

(S 4 0 0)。管理サーバ 1 0 0 では、識別番号 3 5 0 から携帯端末 1 0 の所有者の個人データをチェックする。さらに、ブラックリストのチェックを行う (S 5 0 0)。

あるいは、一度受信したブラックリストを自動販売機 9 0 に記憶しておき、
5 自動販売機 9 0 でチェックを行うようにすることも可能である。これにより、管理サーバ 1 0 0 との送受信の時間に要する時間を短縮し、利便性を高めることも可能である。

以下、自動販売機 9 0 と管理サーバ 1 0 0 とは、サーバ接続部 8 0 から送受信されるものとする。

10 自動販売機 9 0 では、管理サーバ 1 0 0 でのチェック結果より個人データ及びブラックリストに問題がある場合は (S 4 0 0)、携帯端末 1 0 に購入不可を発信する。携帯端末 1 0 には使用不能を表す画面 1 0 0 7 を表示する (S 3 0 2)。

また、個人データ及びブラックリストに問題が無ければ (S 4 0 0)、携
15 帯端末 1 0 に購入許可を発信する。携帯端末 1 0 には商品の選択画面 1 0 0 4 を表示する (S 3 0 3)。

自動販売機 9 0 で商品を選択すると (S 4 0 1)、自動販売機 9 0 から携帯
端末 1 0 に商品代金の引き落としデータが送られる (S 4 0 2)。携帯端
末 1 0 では、代金減算処理が行われ、処理中の画面 1 0 0 5 が表示される (S
20 3 0 4)。さらに、このとき携帯端末 1 0 から代金引き落としの処理が正常に行われなかった場合には (S 4 0 2)、利用情報として NG の通知が自動販売機 9 0 から管理サーバ 1 0 0 に送信され、個人データまたはブラックリストが更新される (S 5 0 1)。

自動販売機 9 0 では、携帯端末 1 0 から代金引き落としの処理が正常に行
25 われたが (S 4 0 2)、商品の払い出しが正常に行われなかった場合には (S 4 0 3)、利用情報として NG の通知を自動販売機 9 0 から管理サーバ 1 0 0 に送信され、正常に動作しなかった自動販売機 9 0 の装置番号 9 1 が記録される (S 5 0 2)。

また、携帯端末 1 0 から代金引き落としの処理が正常に行われ (S 4 0 2)、

さらに、商品の払い出しが正常に行われた場合には（Ｓ４０３）、購入処理完了を自動販売機９０から携帯端末１０に発信する。携帯端末１０では残金が画面１００６に表示される。（Ｓ３０５）。さらに、利用情報として購入情報が自動販売機９０から管理サーバ１００に送信され、履歴として記録される（Ｓ５０３）。
5

ここでは、携帯端末１０について説明したがＩＣカード５０でも同様に行うことができる。

また、自動販売機９０から商品が正常に払い出しされなかった場合には、携帯端末１０の通信回線送信部２５より通信回線１１０を介して管理サーバ１００に接続して、携帯端末１０の識別番号３５０と自動販売機９０を利用した利用情報とをともに、装置番号９１よりどの自動販売機９０を利用したかが確認でき、代金の払い戻しを受けることも可能である。
10

さらに、自動販売機９０の装置番号９１を携帯端末１０のＲＦＩＤインターフェースの送受信部２０を介して受信し、利用情報と携帯端末１０の識別情報３５０と装置番号９１とを、携帯端末１０の通信回線送信部２５より通信回線１１０を介して管理サーバ１００に送信することも可能である。
15

ここでは、携帯端末１０をプリペイドカードとして利用した場合について説明したが、携帯端末１０をキャッシュカード・デビットカード・ポイントカード・スマートカードクレジットカードなどとして利用した場合でも同様に行える。
20

また、ここでは情報はセキュリティ上、暗号化されて管理サーバに送信されることが好ましい。

以上、説明したように、携帯端末１０に一意に割り振られる識別情報３５０と利用情報を関連付けて管理することにより携帯端末１０の利用履歴をとることができる。
25

携帯端末１０にＧＰＳ（Global Positioning System）機能を備え、位置情報を取得して携帯端末１０の位置を正確に把握することにより、装置番号９１とを比較することで不正利用を防ぐことが可能である。

さらに、図２９に示す利用管理システム１４'のように、携帯端末１０を

使用する際、第 3 の実施の形態で説明したように携帯端末 10 の使用者が正当な使用者かをレッドバッジ 70 で確認を取るようにすることも可能である。

5 これにより、正当な携帯端末 10 の利用者のみ携帯端末 10 を使用することができ。

第 6 の実施の形態では、インターネットなどの回線を利用して携帯端末 10 や IC カード 50 にキャッシュカードやプリペイドカードの機能を登録する第 2 の利用管理システムについて説明する。前述の実施の形態と同一のものには同一符号を伏して詳細な説明を省略する。

10 第 6 の実施の形態における利用管理システム 15 は、図 30 に示すように、携帯端末 10 や IC カード 50 と R F I D インターフェースの送受信部 20 を組み込んだ装置 90' と管理サーバ 100 とが通信回線 110 を介して接続される。さらに、通信回線 110 には、銀行の端末やネットバンクなどの金融機関 120 が接続される。

15 装置 90' は、R F I D インターフェースの送受信部 20 を備えたプリペイド購入機 90' とし、携帯端末 10 や IC カード 50 に対して、プリペイドカードの残高の書換が行われるものを例に説明する。さらに、装置 90' には、装置毎に割り振られる装置番号 91 を記録している。

20 次に、本実施の形態の動作を図 31 のフローチャートと図 32 の携帯端末 10 の画面の遷移図に従って説明する。

まず、携帯端末 10 では、図 32 の画面の遷移図に示すように、メニューからプリペイドカードのモード 1100 ~ 現金加算モード 1101 を選択する (S 310)。ここで、識別情報 350 を R F I D インターフェースで携帯端末 10 からプリペイド購入機 90' に発信すると、携帯端末 10 には、
25 個人認証中の画面 1102 が表示される (S 311)。

プリペイド購入機 90' では、識別情報 350 を受け取ると、携帯端末 10 の識別情報 350 をサーバ接続部 80 から管理サーバ 100 に送信して、残高確認及びブラックリストとの照合を行う (S 410)。管理サーバ 100 では、識別番号 350 から携帯端末 10 の所有者の個人データをチェック

する。さらに、ブラックリストのチェックを行う（S 5 1 0）。以下、プリペイド購入機 9 0' と管理サーバ 1 0 0 とは、サーバ接続部 8 0 から送受信されるものとする。

5 プリペイド購入機 9 0' では、個人データ及びブラックリストに問題がある場合は（S 4 1 0）、携帯端末 1 0 に加算不可を発信する。携帯端末 1 0 では加算不能を表す画面 1 1 0 6 を表示する（S 3 1 2）。

10 また、個人データあるいはブラックリストに問題が無ければ（S 4 1 0）、携帯端末 1 0 に購入許可を発信する。携帯端末 1 0 には加算金額の選択画面 1 1 0 3 を表示する（S 3 1 3）。プリペイド購入機 9 0' では、加算金額が選択される（S 4 1 1）と携帯端末 1 0 に加算金額のデータを送る（S 4 1 2）。

15 ここで、指定された金額が金融機関 1 2 0 に残高があるかを確認し（S 4 1 2）、不足の場合は、携帯端末 1 0 に残金不足を発信して残金不足のエラー画面 1 1 0 7 を表示する（S 3 1 4）。不足に問題がない場合は、加算処理が行われ、処理中の画面 1 1 0 4 が表示される（S 3 1 5）。さらに、このとき携帯端末 1 0 から加算処理が正常に行われなかった場合には（S 4 1 3）、利用情報として N G の通知が管理サーバ 1 0 0 に送信され、個人データにエラーが記録される（S 5 1 1）。さらに、携帯端末 1 0 には加算処理異常のエラー画面 1 0 0 8 が表示される（S 3 1 6）。

20 携帯端末 1 0 から加算処理が正常に行われた場合には（S 4 1 3）、残高が携帯端末 1 0 の画面 1 1 0 8 に表示され（S 3 1 7）、利用情報として加算情報とプリペイド購入機 9 0' の装置番号 9 1 とが管理サーバ 1 0 0 に送信され履歴として記録される（S 5 1 2）。

25 また、銀行などの金融機関 1 2 0 から引き落として携帯端末 1 0 に加算処理をする例について説明したが、プリペイド購入機 9 0' に現金を投入して携帯端末 1 0 に加算処理をすることも可能である。

さらに、自動販売機 9 0 をプリペイドカード購入機 9 0' として利用することも可能である。

ここでは、携帯端末 1 0 をプリペイドカードとして利用した場合について

説明したが、キャッシュカード・デビットカード・クレジットカード・会員権・診察券・健康保健所・身分証明書・アミューズメント施設のチケット類などでも同様におこなうことが可能である。

また、本実施の形態では、RFIDインターフェースをもつ専用機 90' を例に説明したが、金融機関 120 から通信回線 110 を介して直接引き落として携帯端末 10 に加算処理をし、さらに、管理サーバ 100 へ携帯端末 10 の識別情報 350 と利用情報と送信するようにすることもできる。

各種クレジット会社との通信回線 110 を介して送受信することにより、クレジットカードの機能を携帯端末 10 に追加することも可能である。

10 以上、説明したように、携帯端末 10 にカードなどの機能を持たせることができ、さらに、識別番号 350 から携帯端末 10 に登録されている全ての利用状況を管理することができる。

さらに、図 33 に示す利用管理システム 15' のように、携帯端末 10 に加算処理をする際に、第 3 の実施の形態で説明したように携帯端末 10 の使用者が正当な使用者かをレッドバッジ 70 で確認を取るようにすることも可能である。

これにより、正当な携帯端末 10 の利用者のみ携帯端末 10 に加算処理をすることができる。

第 7 の実施の形態では、RFIDインターフェースを持つ携帯端末 10 同士の送受信について説明する。前述の実施の形態と同一のものには同一符号を伏して詳細な説明を省略する。

図 34 に示すように、携帯端末 10 と携帯端末 10 とを近づけることにより RFIDインターフェースを使用して送受信を行うことが可能である。例えば、デジタルマネー・着メロ・待ち受け画面などのデジタル情報を相手側の携帯端末 10 に渡すことが可能である。

以上詳細に説明したように、本発明では、携帯端末に定期券・クレジットカード・運転免許書などの個人情報に携帯端末に登録することができる。

また、携帯端末に一意に割り振られる識別情報をもとに携帯端末の利用状況の履歴を取ることが確実に行われ悪用を防ぐことができる。

さらに、携帯端末が悪意を持つ第 3 者に渡っても、対応するレッドバッジ（ＩＣチップ）などがない限り悪用できない。

また、これにより、利用した覚えのない料金を支払う必要がない。

或いは、携帯端末に記憶されている個人データの流出を防ぐことが可能になる。

また、非接触 ＩＣチップとも送受信ができ、携帯端末から ＩＣカードの識別を行うこともできる。さらに、書き込みが行え、容易に ＲＦＩＤシステムが構築できる。

請求の範囲

1. 被保護情報が記録された第 1 アセンブリと、認証情報が記録された第 2 アセンブリとを含む情報保護システムであって、

5 前記第 2 アセンブリは前記第 1 アセンブリからの要求に応じて非接触による情報の送信を可能にする通信手段を備えるものであり、

前記第 1 アセンブリは、

前記被保護情報に対するアクセスを受け付ける受付手段と、

前記認証情報を前記第 2 アセンブリより受け取って認証を行う認証手段

10 と、

この認証手段による認証結果に応じて前記受付手段で受け付けたアクセスを許可又は禁止するアクセス制御手段とを備えるものである、

情報保護システム。

2. 認証用情報と被保護情報とが記録された第 1 アセンブリと、第 2 アセンブリとを含む情報保護システムであって、

前記第 1 アセンブリ及び前記第 2 アセンブリは、それぞれ、他方のアセンブリとの間で非接触による情報の送受信を可能にする通信手段を備えるものであり、

前記第 2 アセンブリは、さらに、前記認証情報を前記第 1 アセンブリより
20 受け取って認証を行う認証手段を備え、

前記第 1 アセンブリは、さらに、

前記被保護情報に対するアクセスを受け付ける受付手段と、

前記第 2 アセンブリから前記認証手段による認証結果を受信するとともにその認証結果に応じて前記受付手段で受け付けたアクセスを許可又は禁止するアクセス制御手段とを備えるものである、
25

情報保護システム。

3. その所有者を認証するための第 1 認証情報と被保護情報とが記録された第 1 アセンブリと、前記所有者を認証するための第 2 認証情報が記録された第 2 アセンブリとを含む情報保護システムであって、

前記第 1 アセンブリ及び前記第 2 アセンブリは、それぞれ、他方のアセンブリとの間で非接触による情報の送受信を可能にする通信手段を備えるものであり、

前記第 2 アセンブリは、さらに、第 1 認証情報を前記第 1 アセンブリより
5 受け取り、受け取った第 1 認証情報と前記第 2 認証情報とに基づく認証を行う第 2 認証手段を備え、

前記第 1 アセンブリは、さらに、

前記被保護情報に対するアクセスを受け付ける受付手段と、

前記第 2 認証情報を前記第 2 アセンブリより受け取り、受け取った第 2 認証情報および前記第 1 認証情報とに基づく認証を行う第 1 認証手段と、
10

前記第 1 認証手段による認証結果および前記第 2 アセンブリより受け取った前記第 2 認証手段による認証結果に応じて前記受付手段で受け付けたアクセスを許可又は禁止するアクセス制御手段とを備えるものである、

情報保護システム。

15 4. 前記第 1 アセンブリ、第 2 アセンブリは、いずれも、単独で携帯可能であるか、または携帯可能な製品に内蔵されていることを特徴とする、請求項 1 記載の情報保護システム。

5. 前記第 1 アセンブリ、第 2 アセンブリは、いずれも、単独で携帯可能であるか、または携帯可能な製品に内蔵されていることを特徴とする、
20 請求項 2 記載の情報保護システム。

6. 前記第 1 アセンブリ、第 2 アセンブリは、いずれも、単独で携帯可能であるか、または携帯可能な製品に内蔵されていることを特徴とする、請求項 3 記載の情報保護システム。

7. 前記通信手段が、電磁誘導による無線通信、電磁結合による無線通信、
25 静電結合による無線通信、及び光を情報の搬送媒体とする通信、のいずれかを行う、

請求項 1 記載の情報保護システム。

8. 前記被保護情報が個人のプライバシーに関わる情報及び/または財的価値に関わる情報である、

請求項 1 記載の情報保護システム。

9. 前記第 1 アセンブリおよび前記第 2 アセンブリが、それぞれ非接触通信のアンテナを含む IC モジュールである、

請求項 1 記載の情報保護システム。

5 10. 前記第 1 アセンブリがカード媒体に埋め込まれたものである、
請求項 1 記載の情報保護システム。

11. 前記第 1 アセンブリがシート状の媒体に埋め込まれたものである、
請求項 1 記載の情報保護システム。

10 12. 前記第 1 アセンブリが携帯性端末に内蔵されたものである、
請求項 1 記載の情報保護システム。

13. 前記第 1 アセンブリがデータキャリアに内蔵されたものである、
請求項 1 記載の情報保護システム。

14. 前記第 2 アセンブリが前記第 1 アセンブリを所持する者が身につける装飾品に埋め込まれたものである、
15 請求項 1 記載の情報保護システム。

15. その所有者を認証するための第 1 認証情報と被保護情報とが記録された第 1 アセンブリと、前記所有者を認証するための第 2 認証情報が記録された第 2 アセンブリと、前記被保護情報を読み取る情報読取装置とを含む情報保護システムであって、

20 前記第 1 アセンブリは、前記第 2 アセンブリおよび情報読取装置との間で非接触による情報の送受信を可能にする第 1 通信手段を備えるものであり、
前記第 2 アセンブリは、前記第 1 アセンブリとの間で非接触による情報の送受信を可能にする第 2 通信手段を備えるものであり、

前記情報読取装置は、前記第 1 アセンブリとの間で非接触による情報の送
25 受信を可能にする第 3 通信手段を備えるものであり、

前記第 1 アセンブリは、さらに、前記情報読取装置からの信号に応答して前記第 2 アセンブリより前記第 2 認証情報を受け取り、受け取った第 2 認証情報および前記第 1 認証情報に基づく認証を行い、認証結果に応じて前記被保護情報の前記情報読取装置による読み取りを許可又は禁止する手段を備

えるものである、

情報保護システム。

16. その所有者を認証するための第1認証情報と被保護情報とが記録された第1アセンブリと、前記所有者を認証するための第2認証情報が記録された第2アセンブリと、前記被保護情報を読み取る情報読取装置とを含む情報保護システムであって、

前記第1アセンブリは、前記第2アセンブリおよび情報読取装置との間で非接触による情報の送受信を可能にする第1通信手段を備えるものであり、

前記第2アセンブリは、前記第1アセンブリとの間で非接触による情報の送受信を可能にする第2通信手段を備えるものであり、

前記情報読取装置は、前記第1アセンブリとの間で非接触による情報の送受信を可能にする第3通信手段を備えるものであり、

前記第2アセンブリは、さらに、前記第1認証情報を前記第1アセンブリより受け取るとともに受け取った第1認証情報および前記第2認証情報に基づく認証を行い、認証結果を前記第1アセンブリに送信する手段を備え、

前記第1アセンブリは、さらに、前記情報読取装置からの信号に応答して前記第2アセンブリに前記第1認証情報を送信するとともに当該第2アセンブリから前記認証結果を受け取り、受け取った認証結果に応じて前記被保護情報の前記情報読取装置による読み取りを許可又は禁止する手段を備えるものである、

情報保護システム。

17. その所有者を認証するための第1認証情報と被保護情報とが記録された第1アセンブリと、前記所有者を認証するための第2認証情報が記録された第2アセンブリと、前記被保護情報を読み取る情報読取装置とを含む情報保護システムであって、

前記第1アセンブリは、前記第2アセンブリおよび情報読取装置との間で非接触による情報の送受信を可能にする第1通信手段を備えるものであり、

前記第2アセンブリは、前記第1アセンブリとの間で非接触による情報の送受信を可能にする第2通信手段を備えるものであり、

前記情報読取装置は、前記第 1 アセンブリとの間で非接触による情報の送受信を可能にする第 3 通信手段を備えるものであり、

前記第 2 アセンブリは、さらに、第 1 認証情報を前記第 1 アセンブリより受け取り、受け取った第 1 認証情報および前記第 2 認証情報に基づく第 2 認証を行うとともに認証結果を前記第 1 アセンブリに送信する第 2 認証手段を備え、

前記第 1 アセンブリは、さらに、

前記情報読取装置からの信号に応答して前記第 2 アセンブリに前記第 1 認証情報を送信するとともに当該第 2 アセンブリから前記第 2 認証情報を受け取り、受け取った第 2 認証情報および前記第 1 認証情報とに基づく第 1 認証を行う第 1 認証手段と、

前記第 1 認証手段による認証結果および前記第 2 アセンブリより受け取った前記第 2 認証手段による認証結果に応じて前記被保護情報の前記情報読取装置による読み取りを許可又は禁止する手段を備えるものである、

15 情報保護システム。

18. 前記第 1 アセンブリ、第 2 アセンブリは、いずれも、単独で携帯可能であるか、または携帯可能な製品に内蔵されていることを特徴とする、

請求項 1 5 記載の情報保護システム。

19. 前記第 1 アセンブリ、第 2 アセンブリは、いずれも、単独で携帯可能であるか、または携帯可能な製品に内蔵されていることを特徴とする、

請求項 1 6 記載の情報保護システム。

20. 前記第 1 アセンブリ、第 2 アセンブリは、いずれも、単独で携帯可能であるか、または携帯可能な製品に内蔵されていることを特徴とする、

請求項 1 7 記載の情報保護システム。

21. 前記第 1 乃至第 3 通信手段が、電磁誘導による無線通信、電磁結合による無線通信、静電結合による無線通信、及び光を情報の搬送媒体とする通信、のいずれかを行う、

請求項 1 5 記載の情報保護システム。

22. 前記被保護情報が個人のプライバシーに関わる情報及び/または財的

価値に関わる情報である、請求項 1 5 記載の情報保護システム。

23. 前記第 1 アセンブリおよび前記第 2 アセンブリが、それぞれ非接触通信用のアンテナを含む IC モジュールである、

請求項 1 5 記載の情報保護システム。

5 24. 前記第 1 アセンブリがカード媒体に埋め込まれたものである、
請求項 1 5 記載の情報保護システム。

25. 前記第 1 アセンブリがシート状の媒体に埋め込まれたものである、
請求項 1 5 記載の情報保護システム。

10 26. 前記第 1 アセンブリが携帯性端末に内蔵されたものである、
請求項 1 5 記載の情報保護システム。

27. 前記第 2 アセンブリが前記第 1 アセンブリを所持する者が身につける装飾品に埋め込まれたものである、

請求項 1 5 記載の情報保護システム。

15 28. それぞれ異なる箇所で独立して存在し、互いの間で非接触による情報の送受信が可能な第 1 アセンブリおよび第 2 アセンブリのうち、第 1 アセンブリに被保護情報を記録しておく、

前記被保護情報へのアクセス要求があったときに、前記第 1 アセンブリとの間で非接触による通信が可能な領域に前記第 2 アセンブリが存在することを条件として、前記第 1 アセンブリが、前記アクセス要求を許可することを特徴とする、
20

情報保護方法。

29. 前記第 1 アセンブリと前記第 2 アセンブリは、いずれも携帯可能な製品に内蔵されていることを特徴とする、

請求項 2 8 記載の方法。

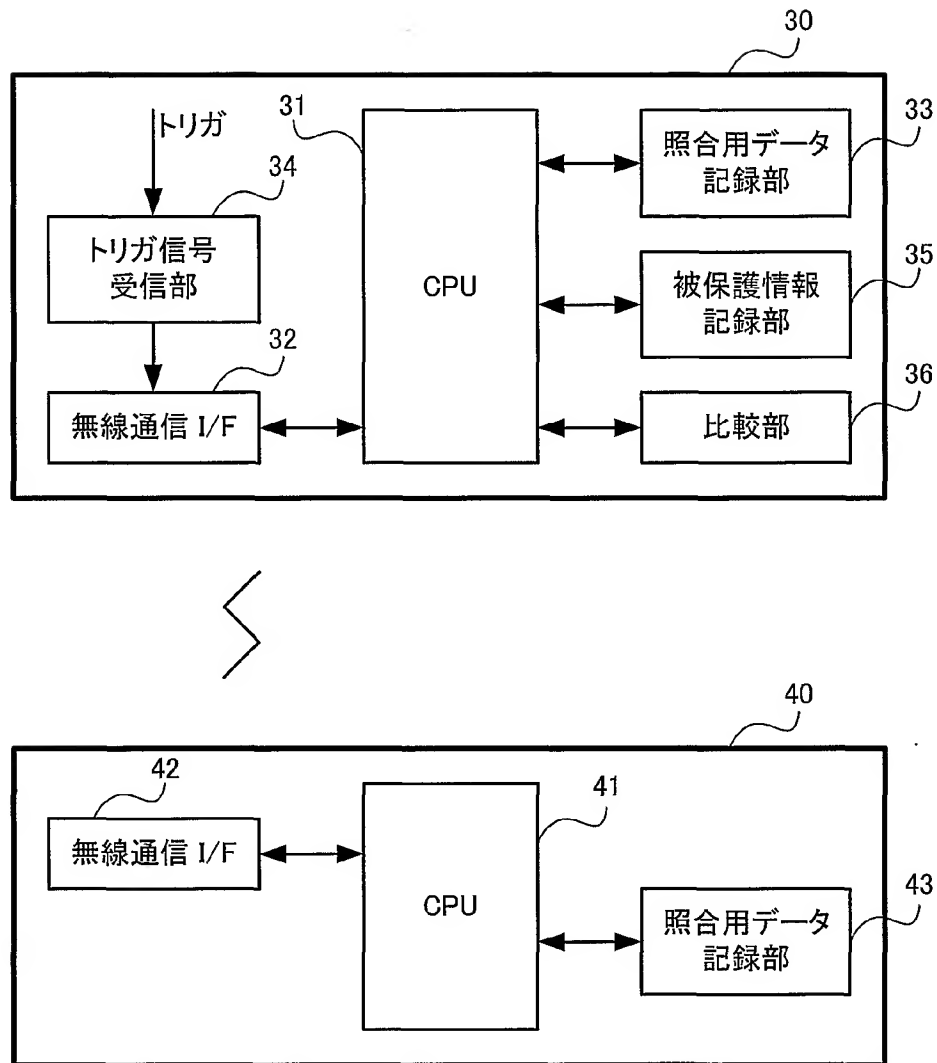
25 30. 前記第 1 アセンブリと前記第 2 アセンブリの少なくとも一方に、前記第 1 アセンブリの所有者を一意に識別するための認証情報を記録しておく、この認証情報に基づく認証の結果、前記所有者であることが確認された場合に、前記第 1 アセンブリが前記アクセス要求を許可することを特徴とする、

請求項 2 8 記載の方法。

31. 前記アクセス制御手段は、当該認証手段でアクセスを許可するという認証結果が得られた場合は、前記アクセス要求から所定時間が経過するまでは、被保護情報へのアクセスを許可することを特徴とする、請求項 1 記載
5 の情報保護システム。

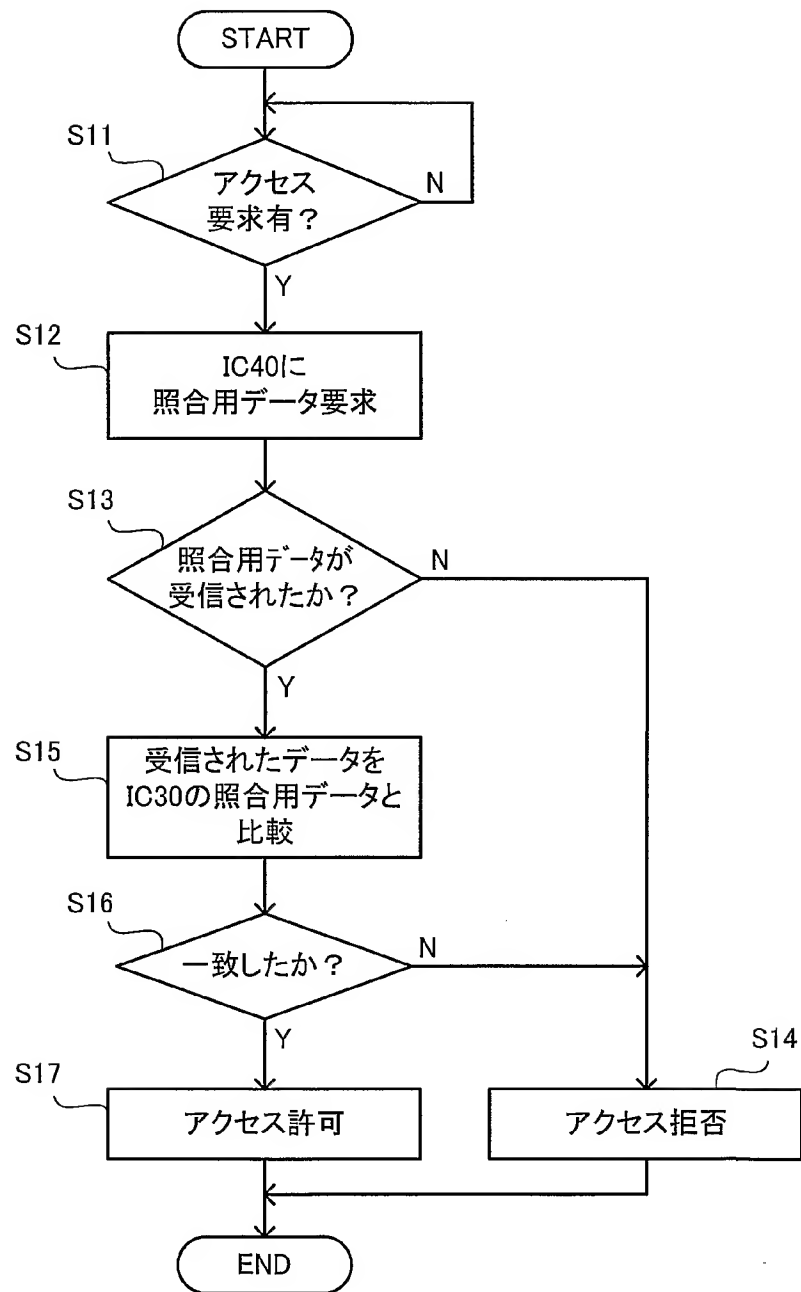
32. 前記アクセス制御手段は、当該認証手段でアクセスを許可するという認証結果が得られた場合は、前記アクセス要求から所定時間が経過するまでは、被保護情報へのアクセスを許可することを特徴とする、請求項 1 5 記載の情報保護システム。

1/32

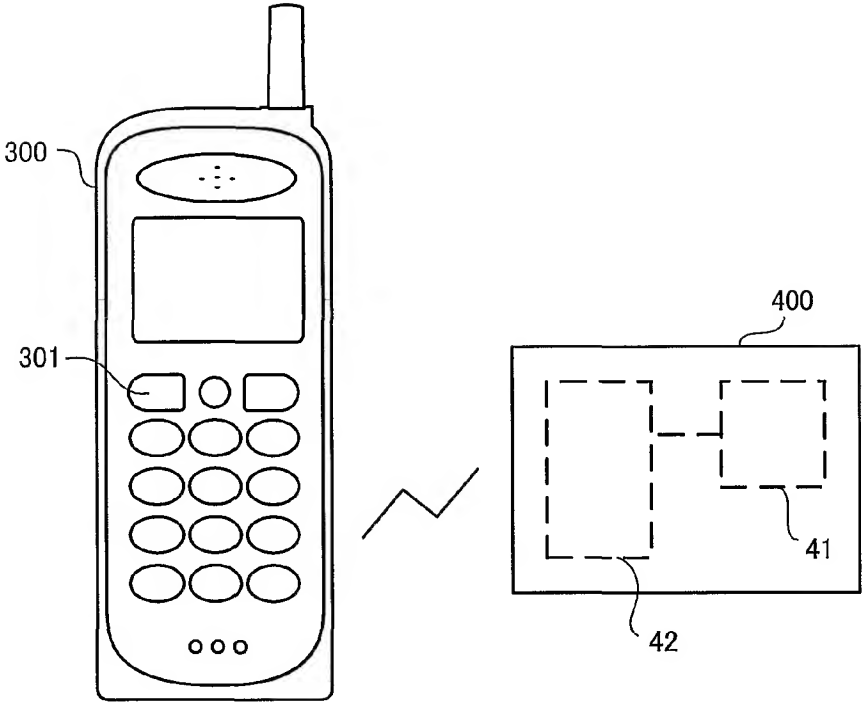


第1図

2/32

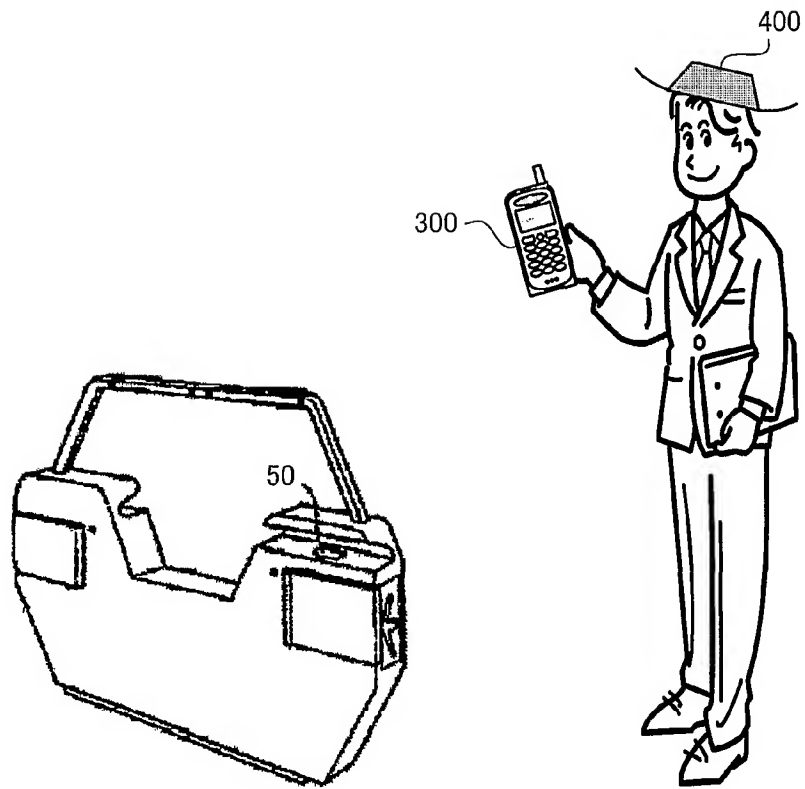


第2図

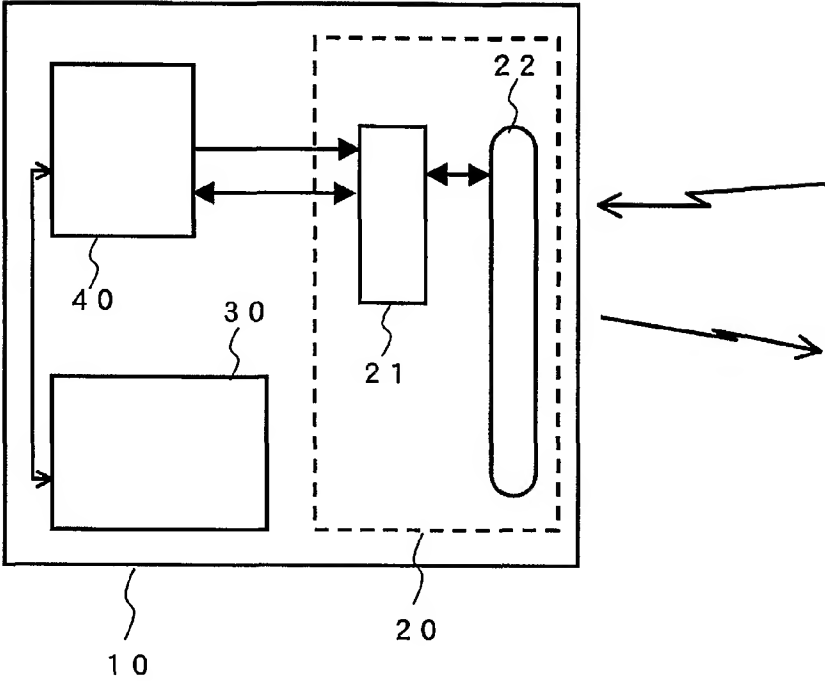


第3図

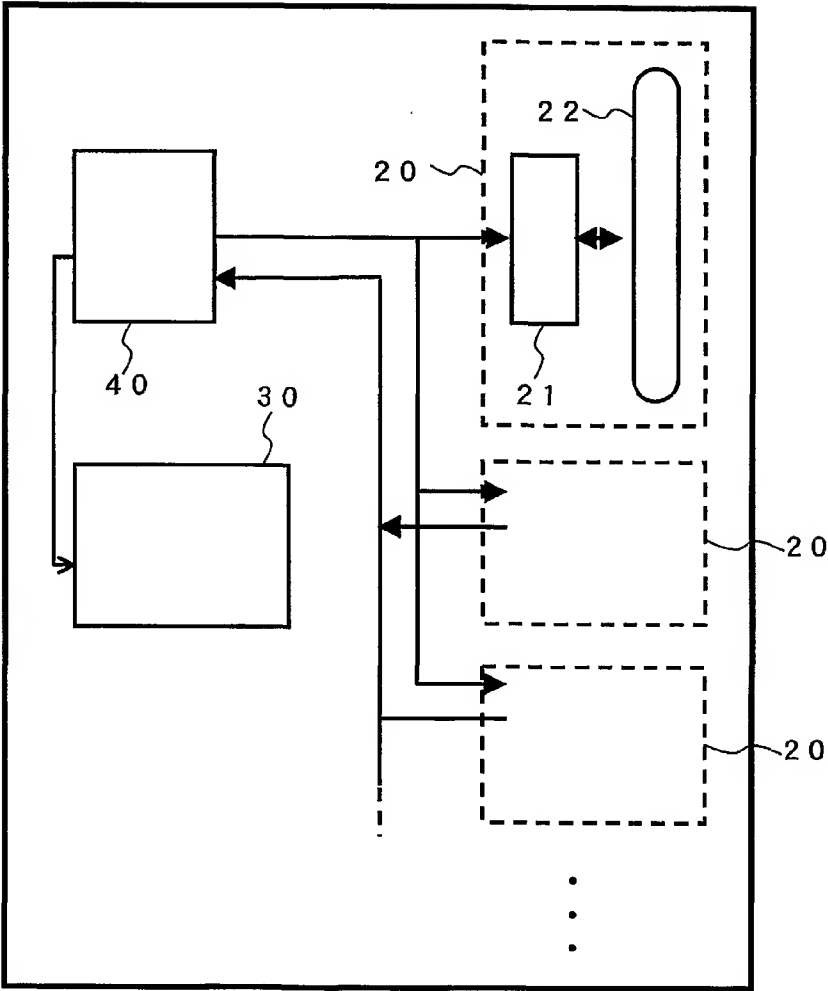
4/32



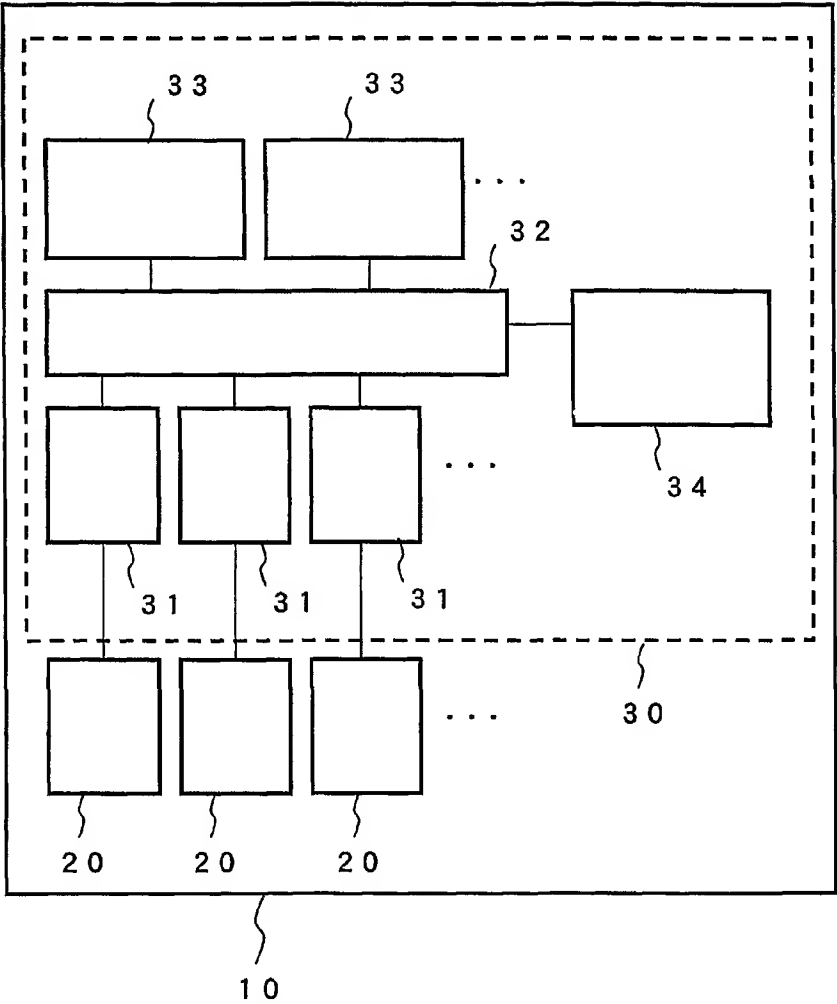
第4図



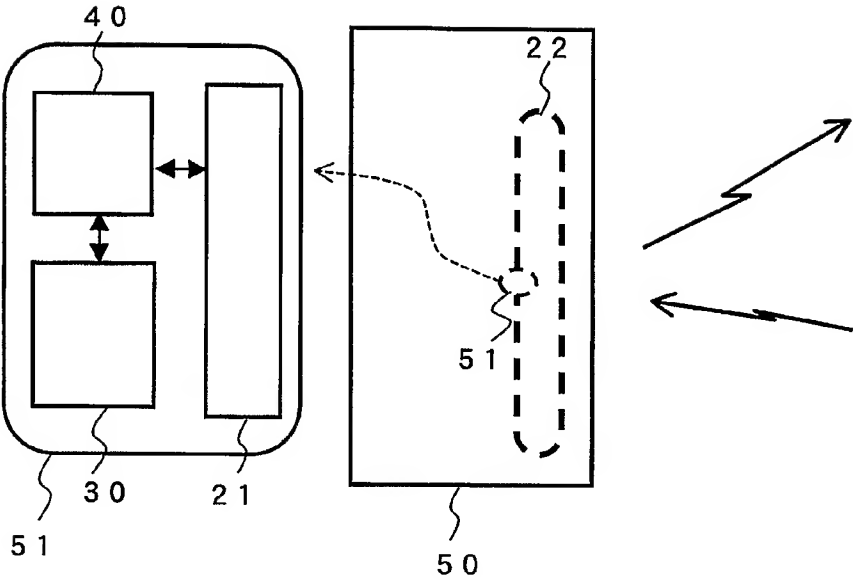
第5図



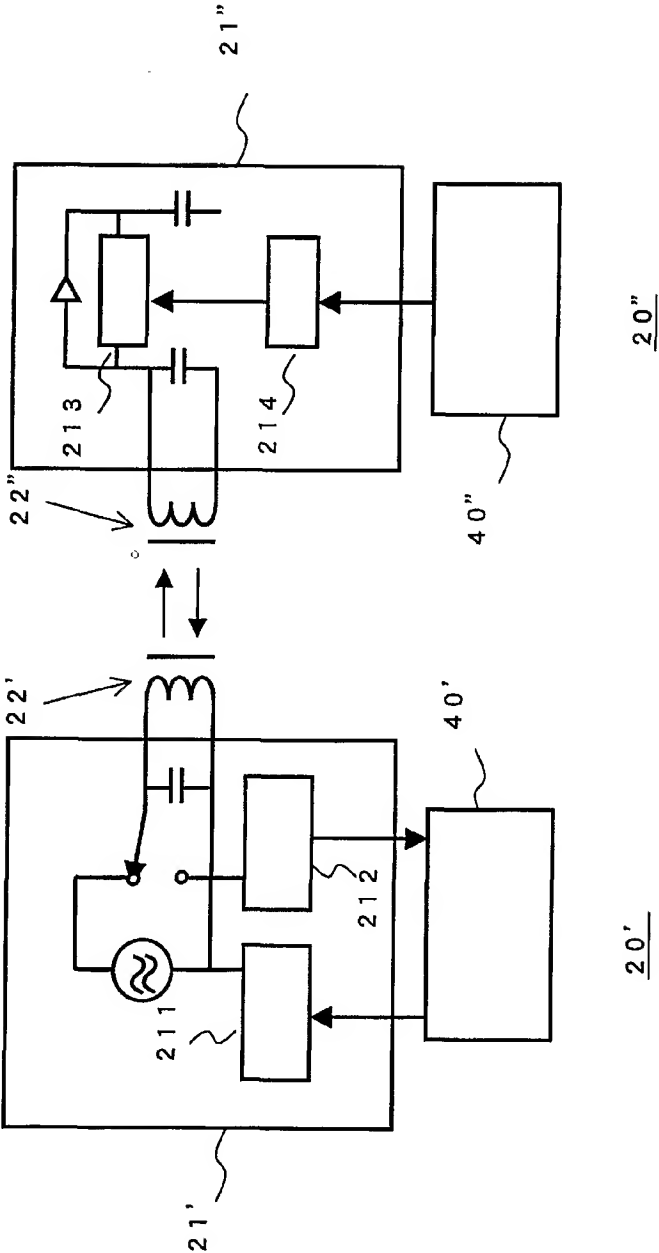
第6図



第7図

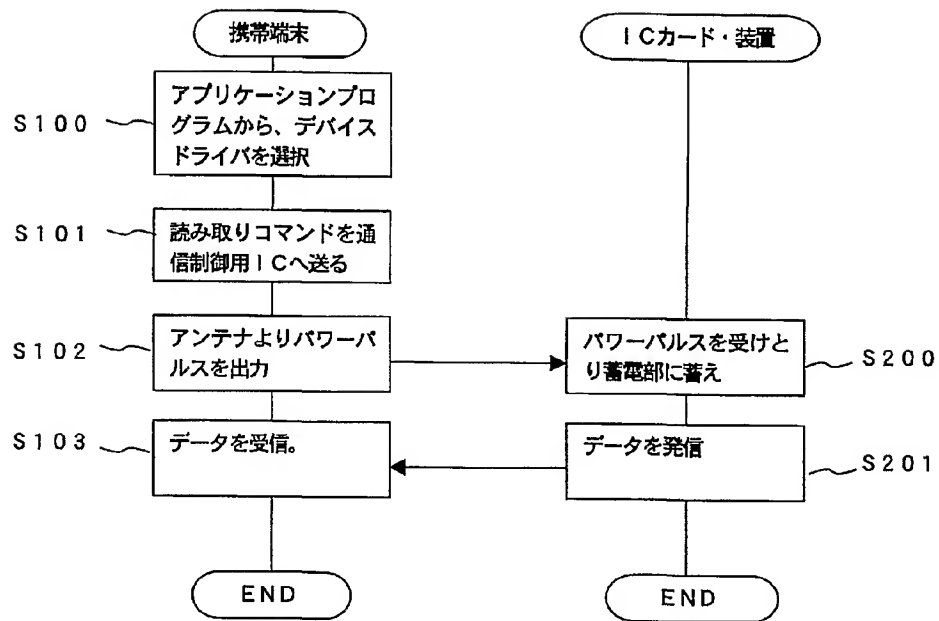


第8図

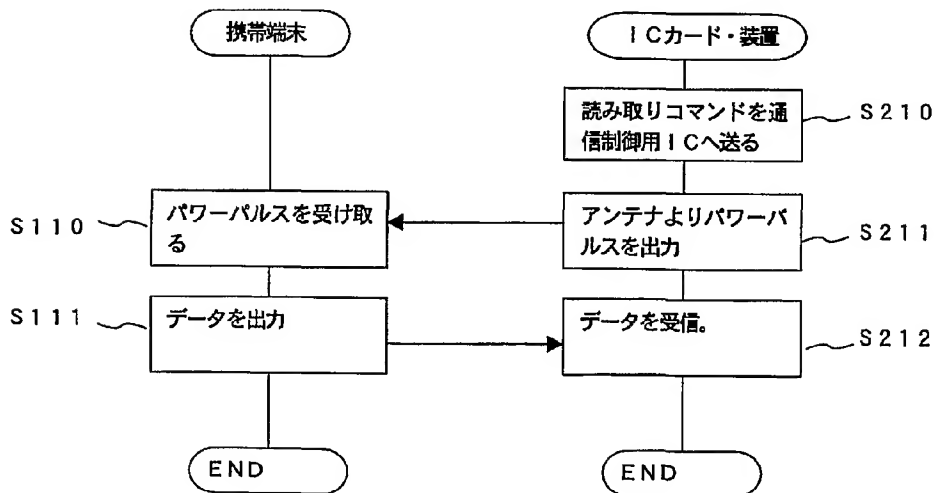


第9図

10/32

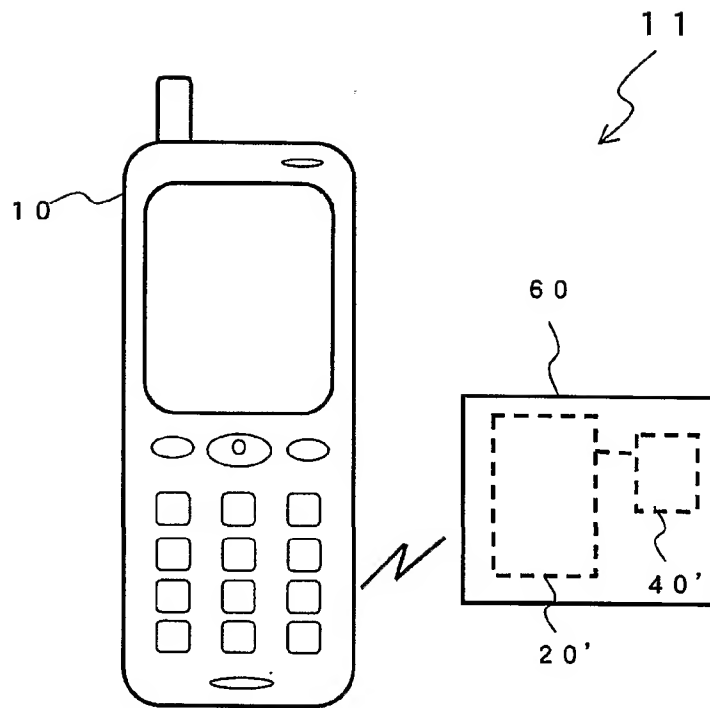


第10図

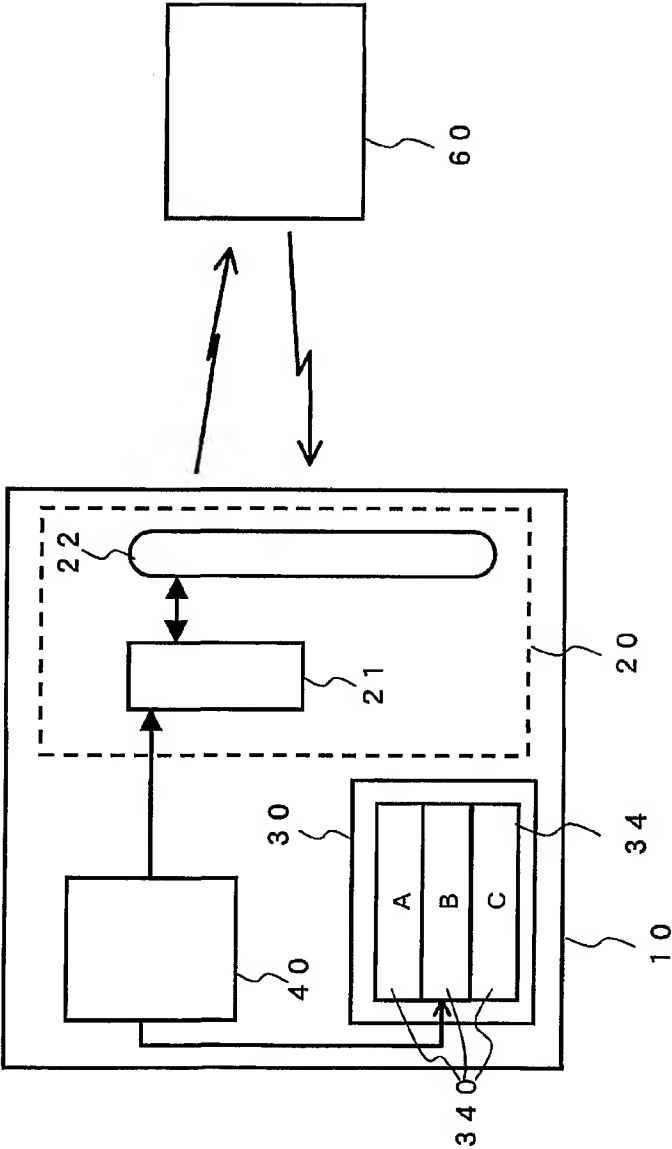


第11図

11/32

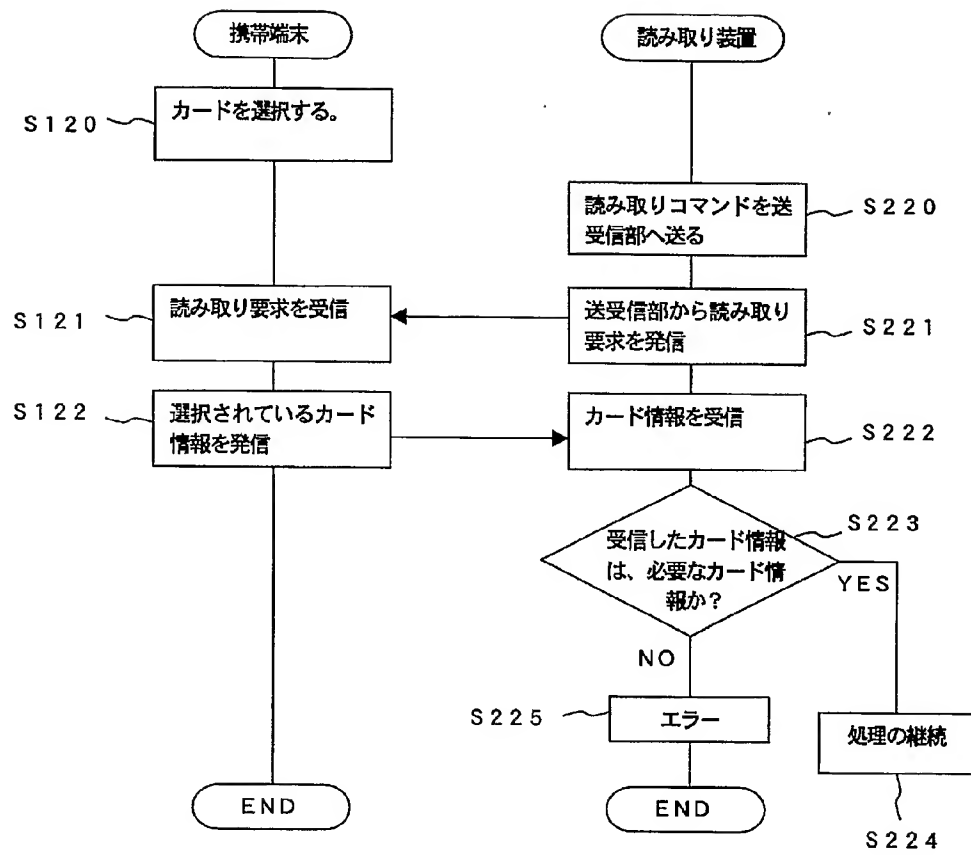


第12図

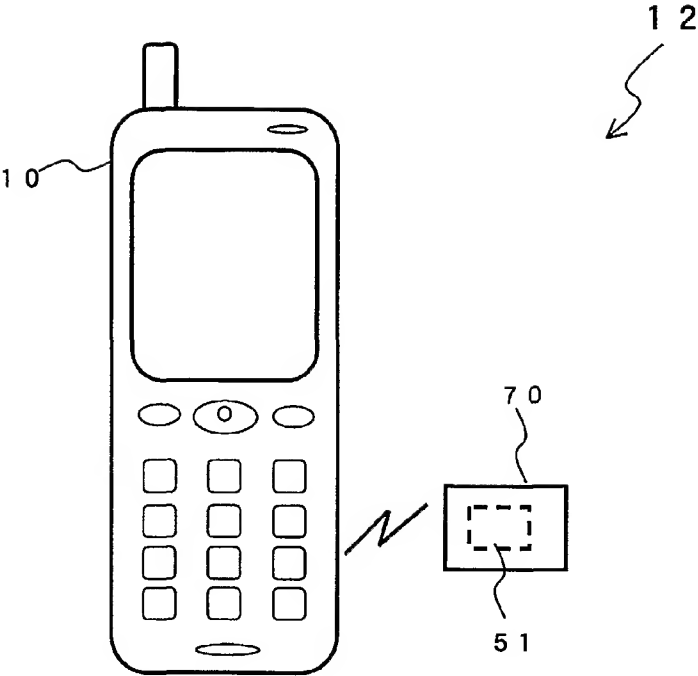


第13図

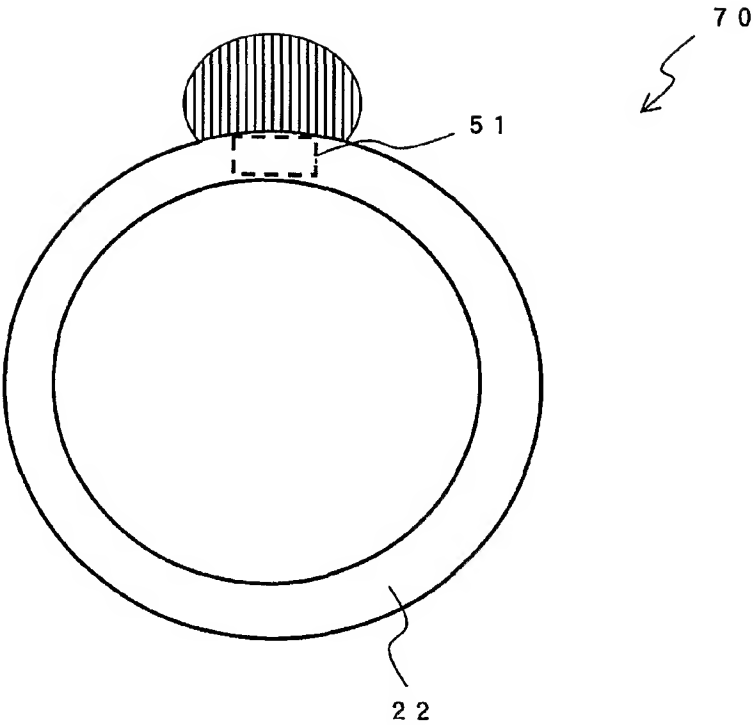
13/32



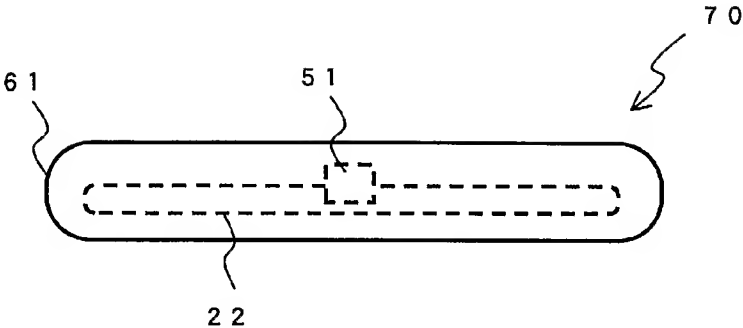
第14図



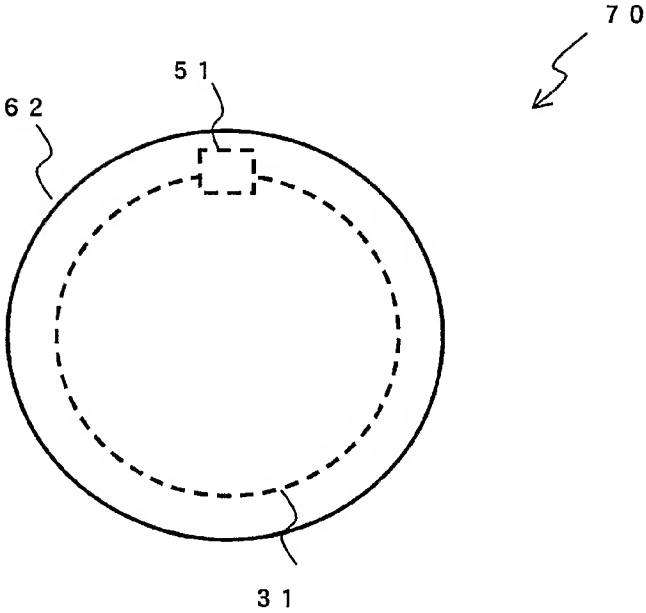
第15図



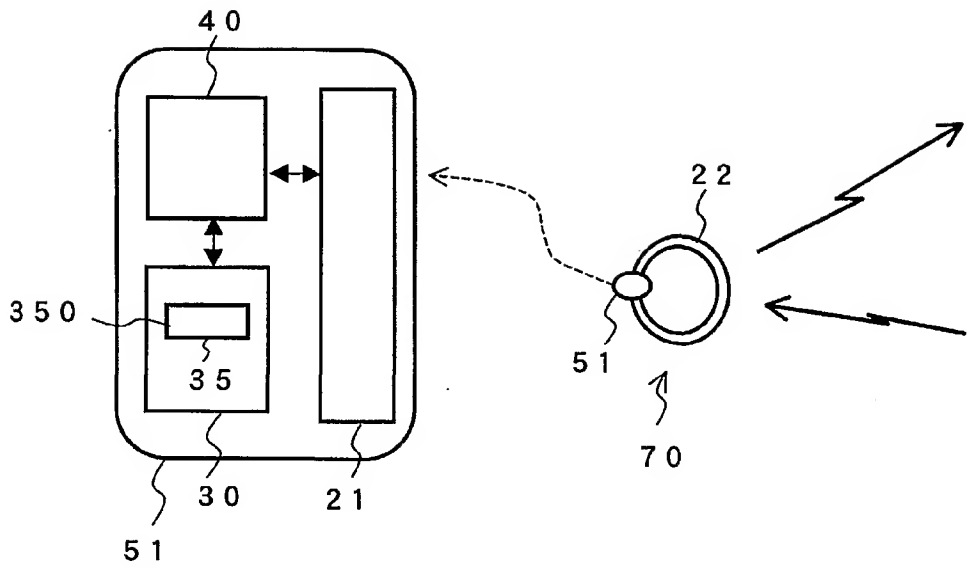
第16図



第17図

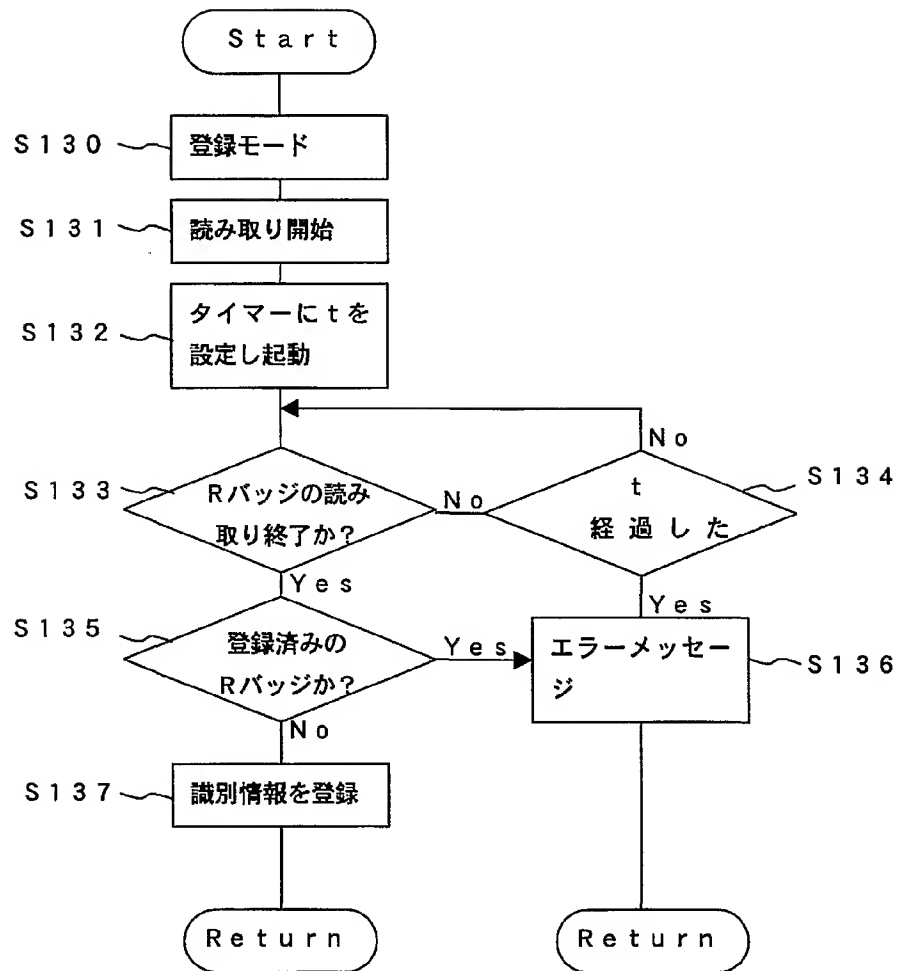


第18図



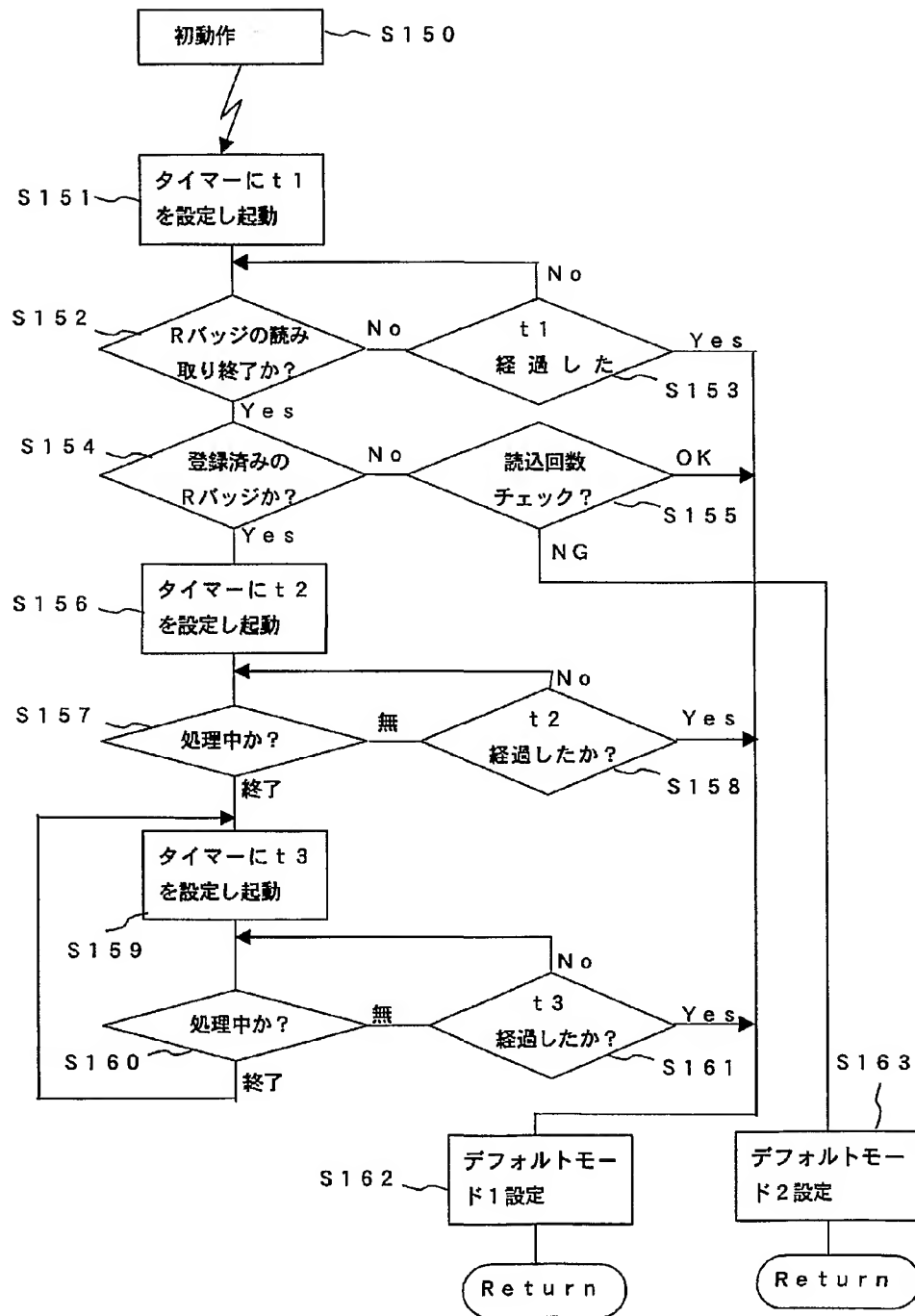
第19図

18/32

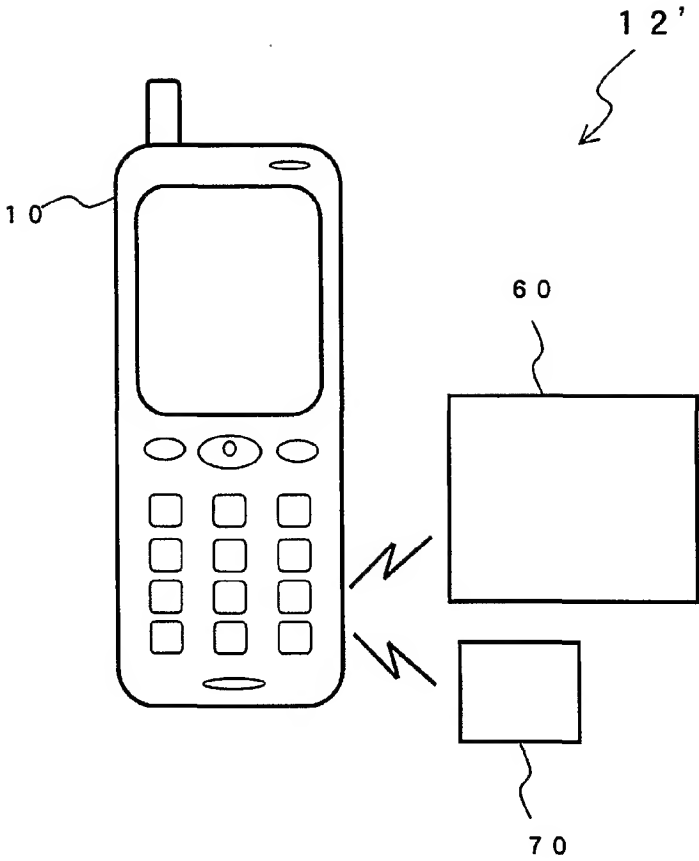


第20図

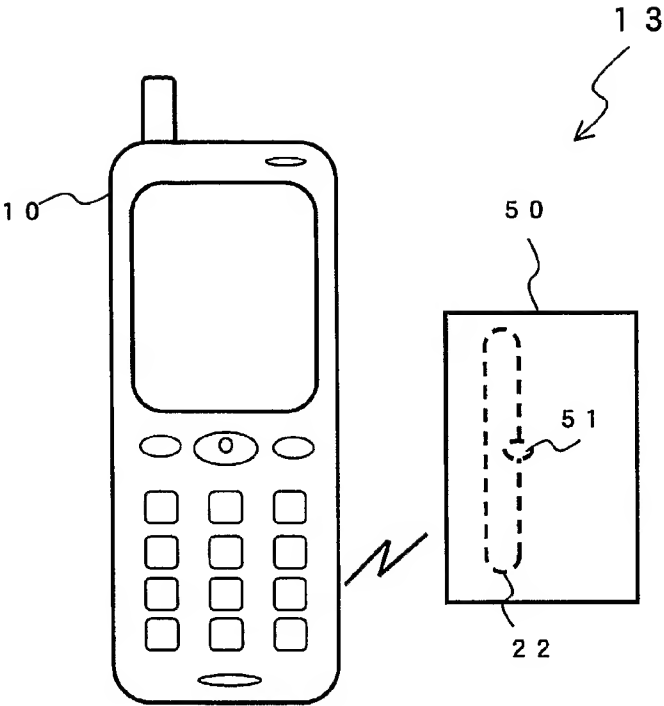
19/32



第21図

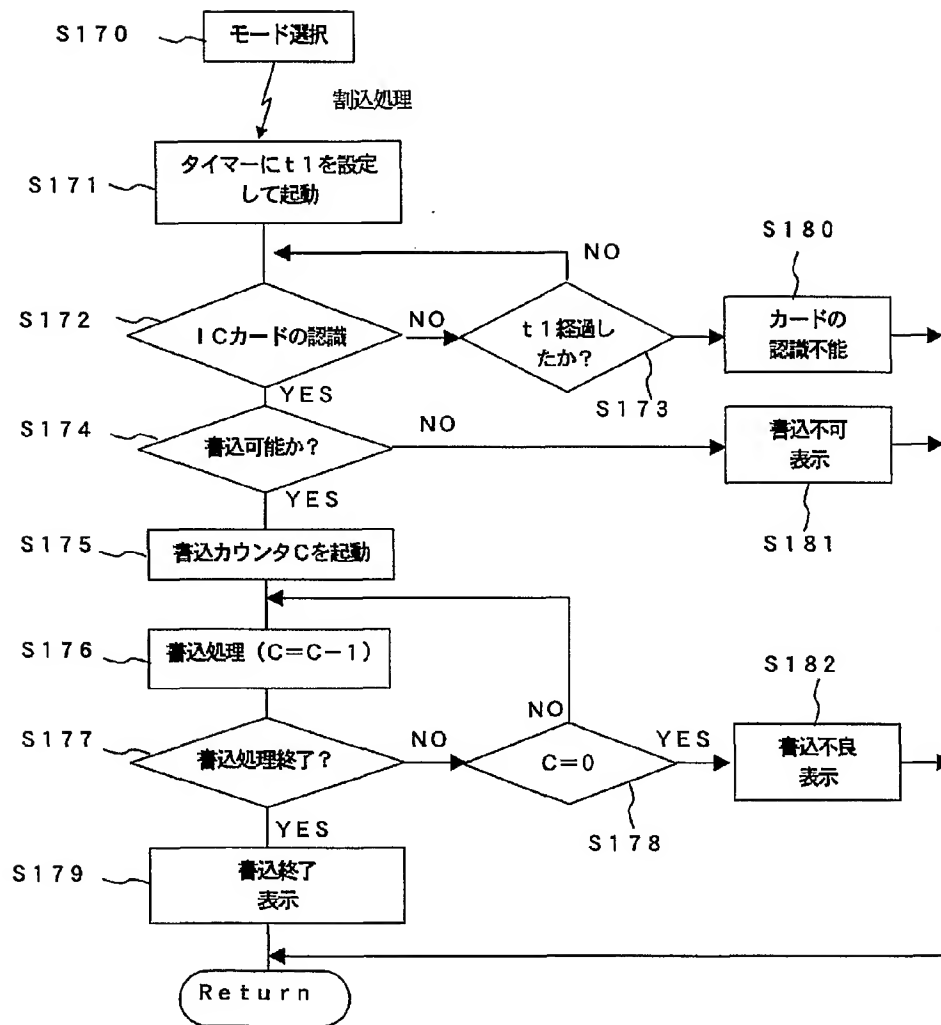


第22図

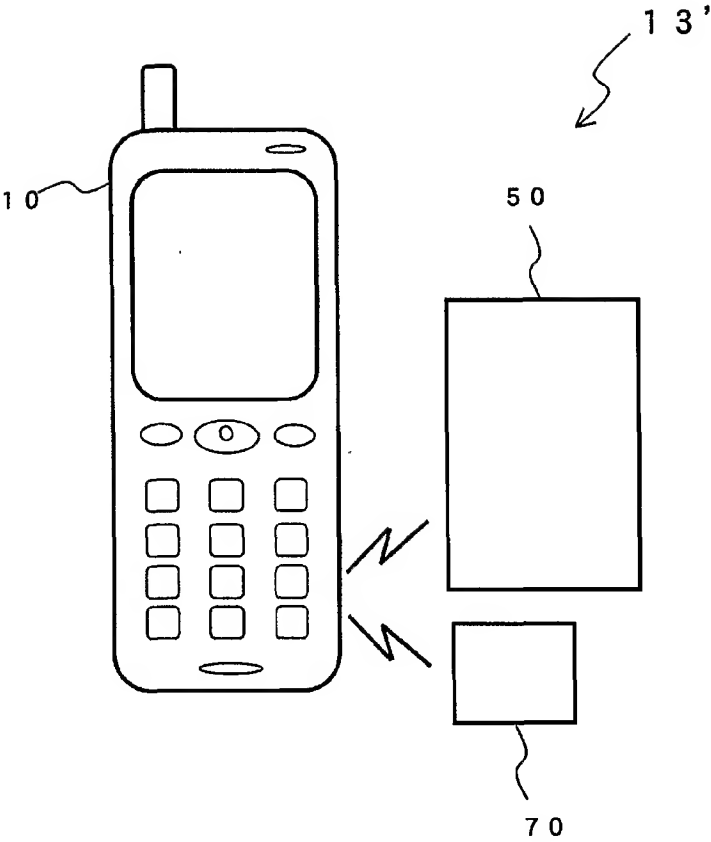


第23図

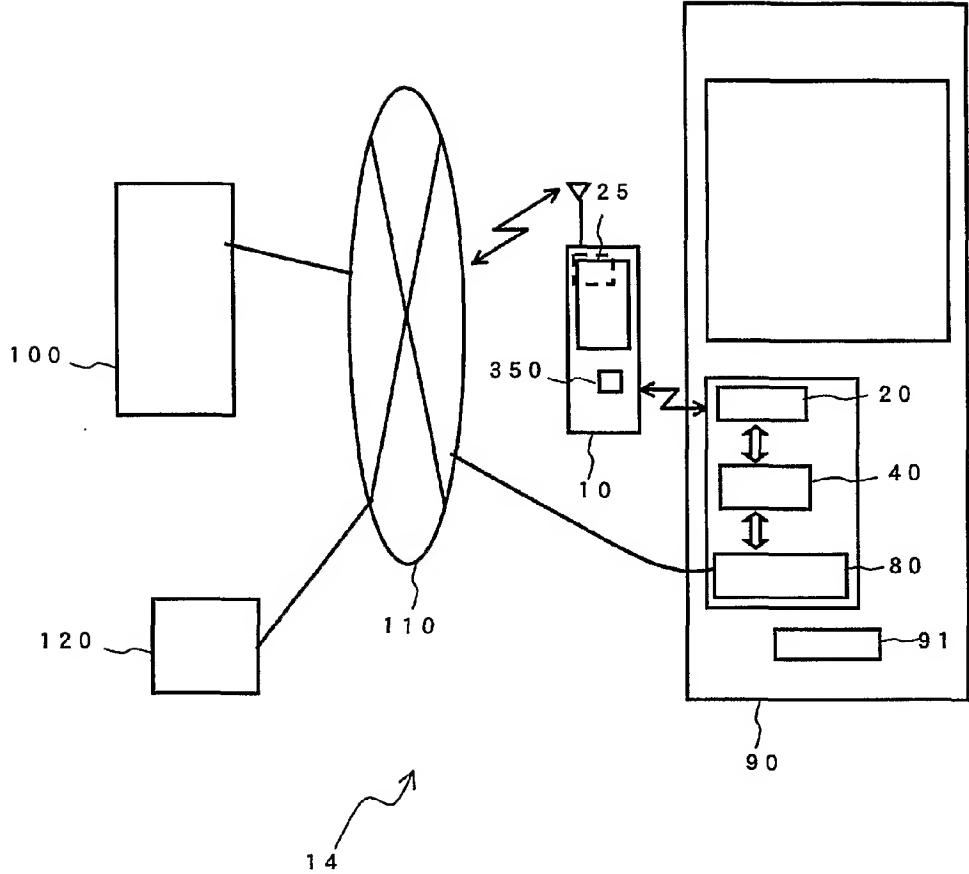
22/32



第24図

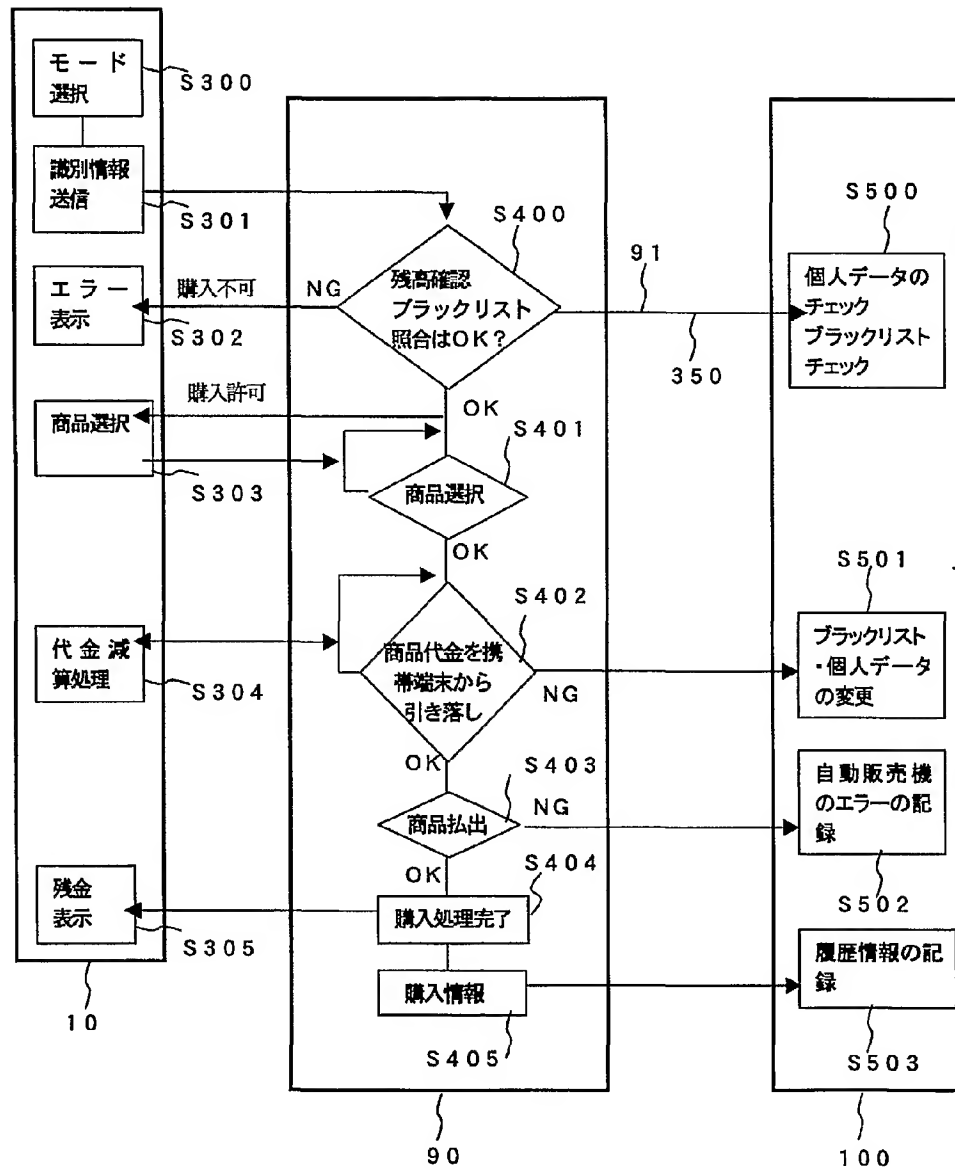


第25図



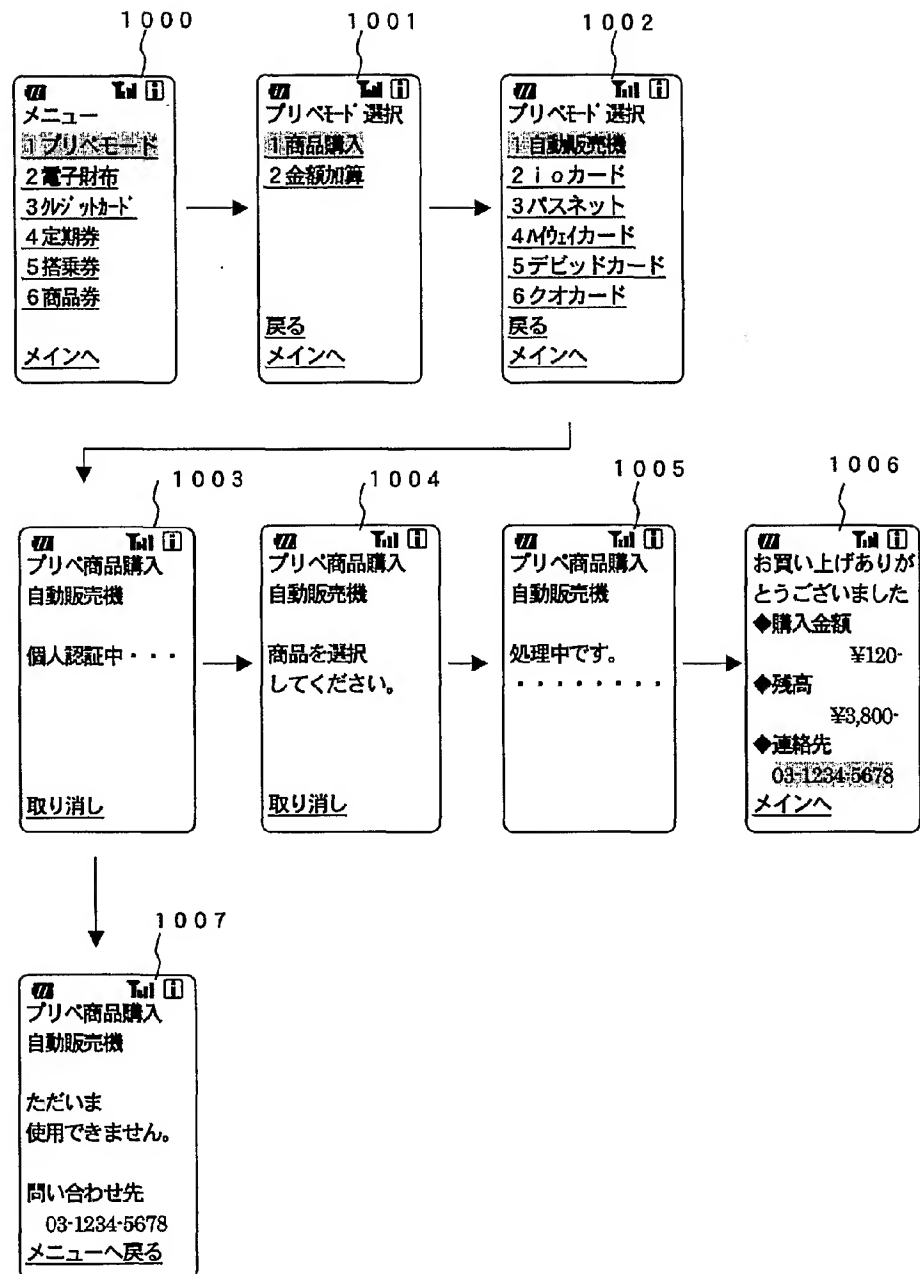
第26図

25/32

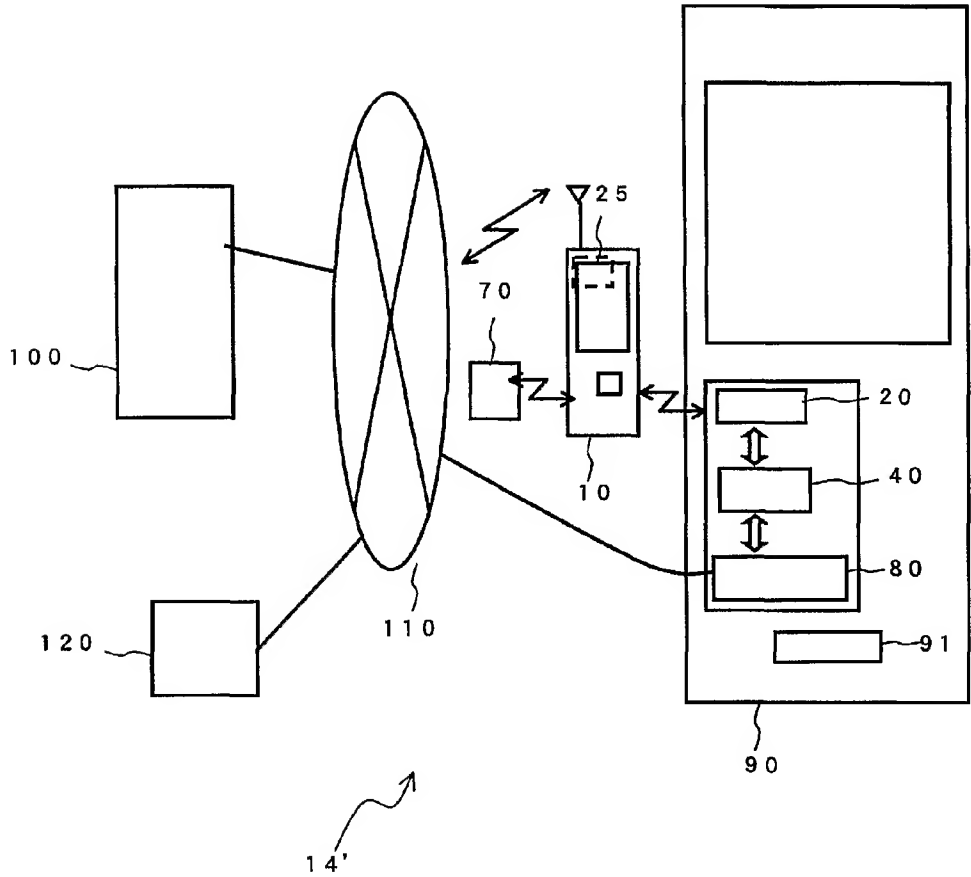


第27図

26/32

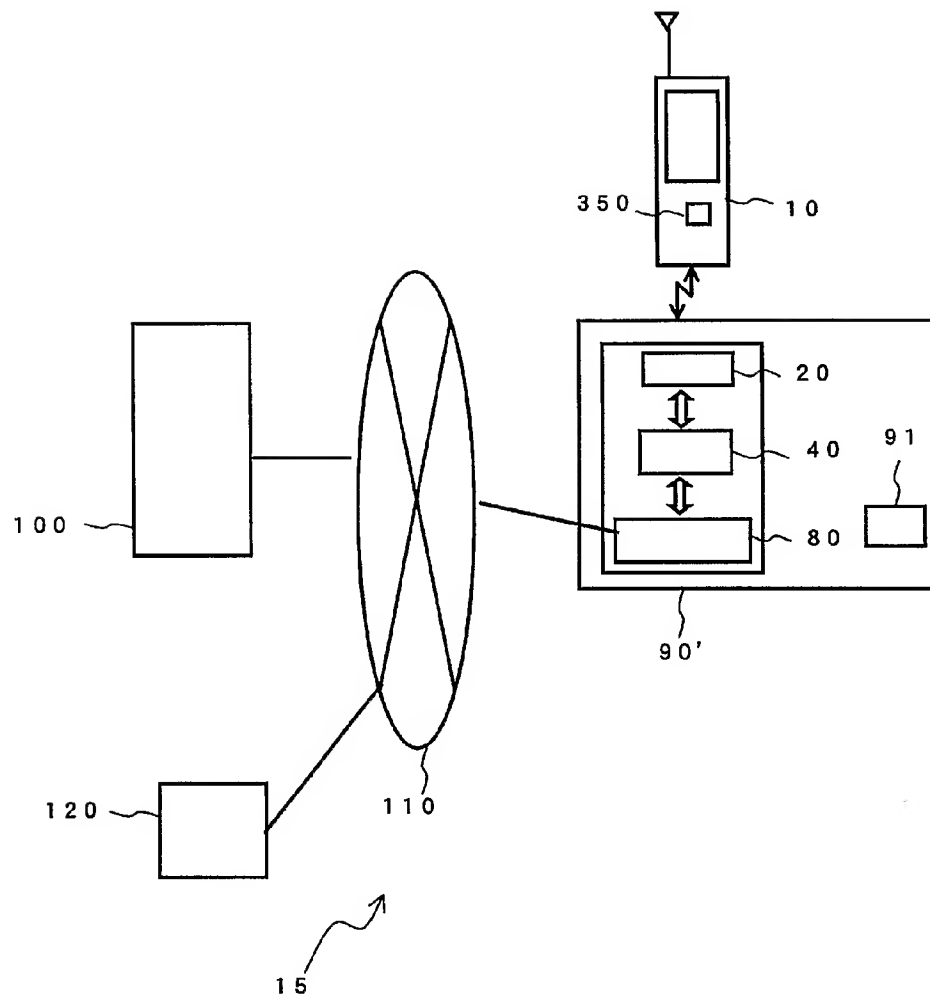


第28図



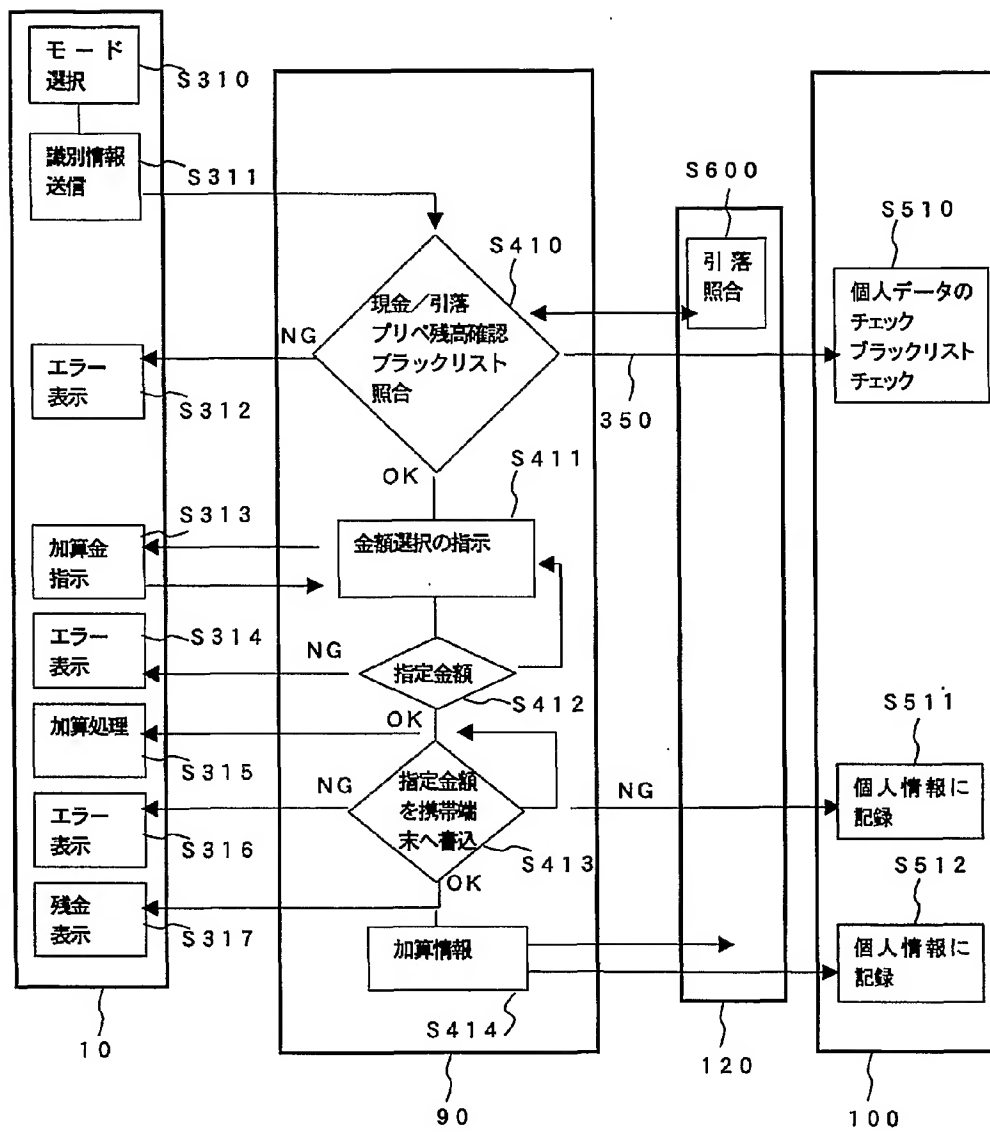
第29図

28/32



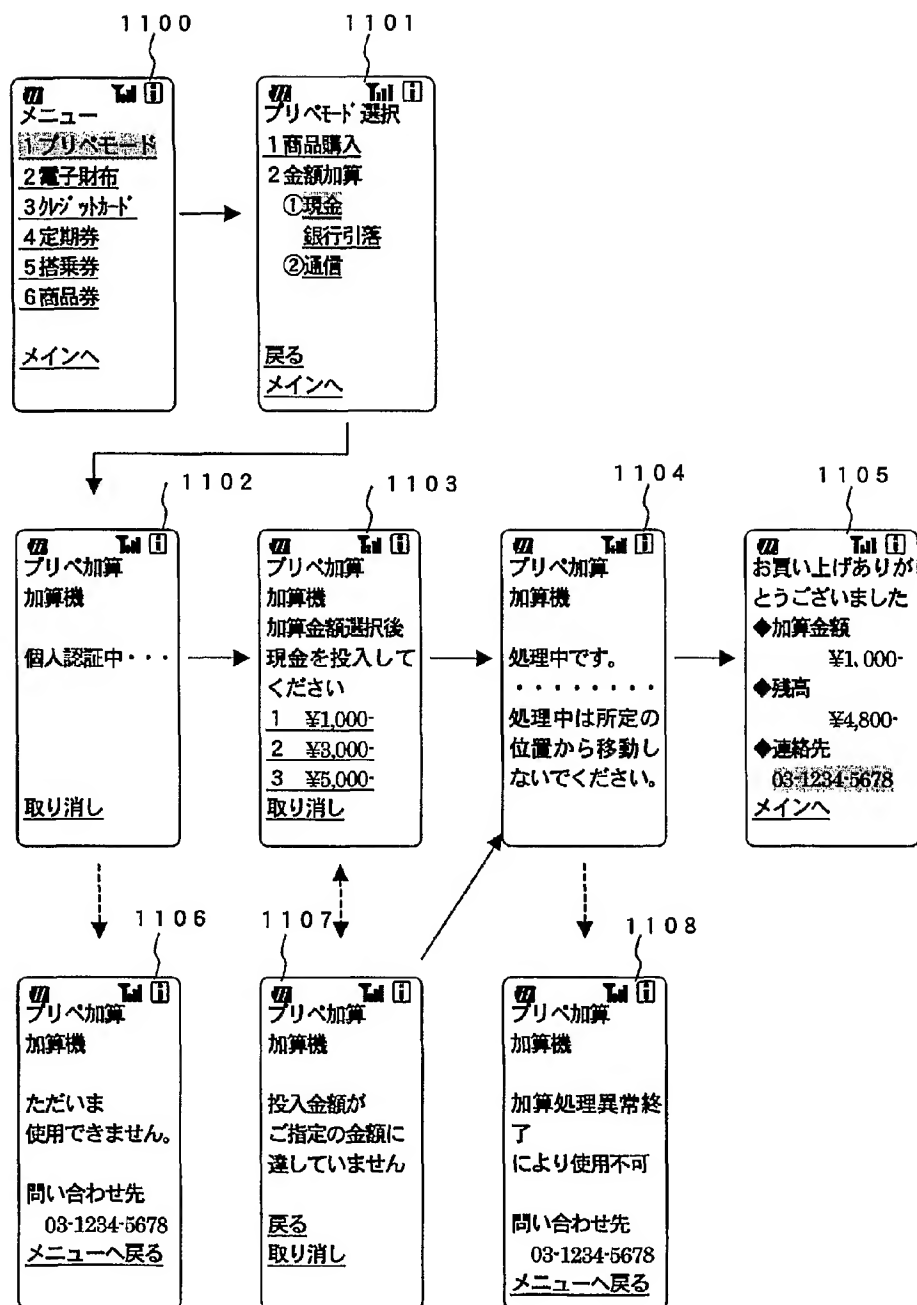
第30図

29/32

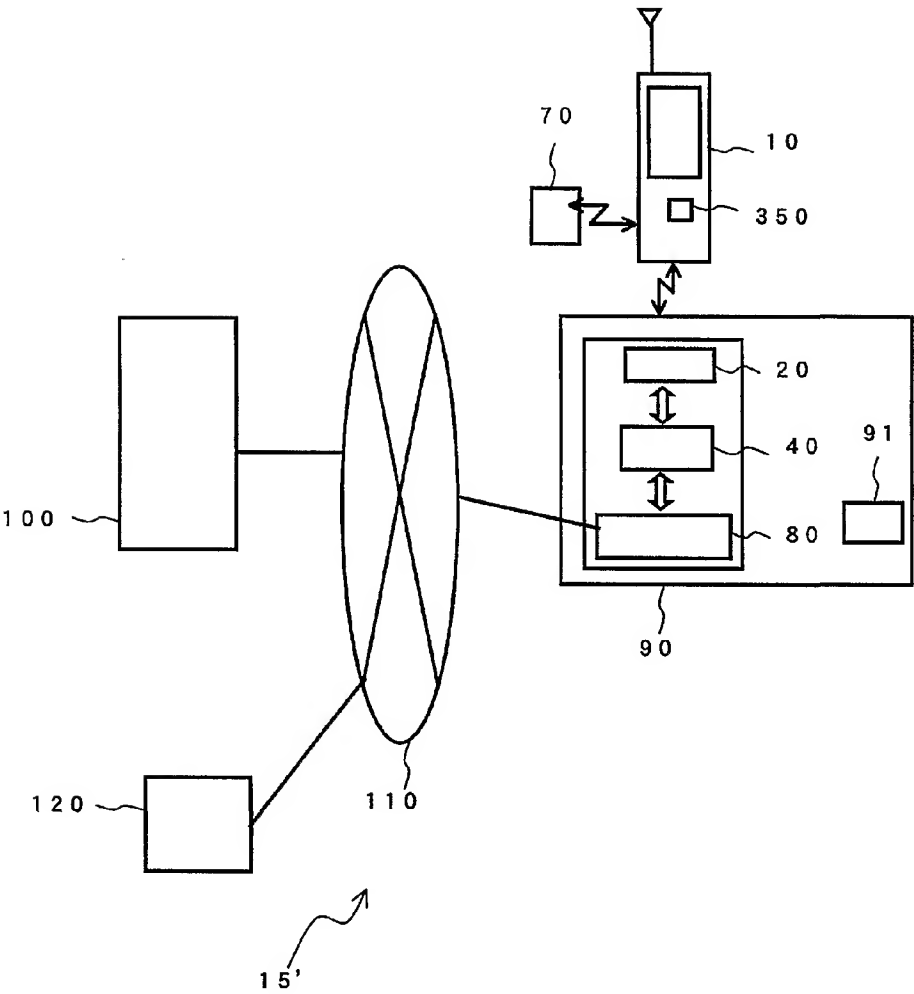


第31図

30/32

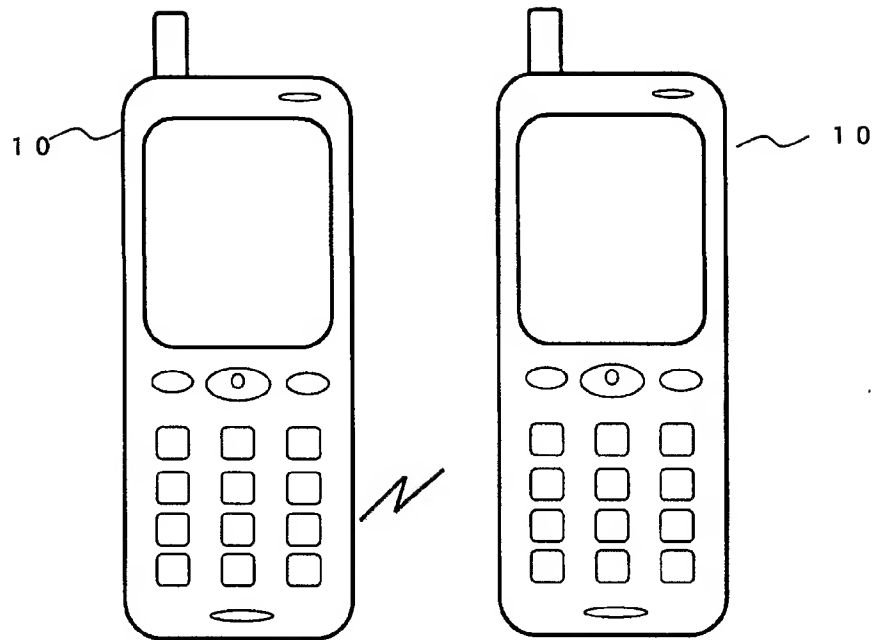


第32図



第33図

32/32



第34図

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/03789

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl.⁷ G06K17/00, 19/073, G06F12/14, 15/00, H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl.⁷ G06K17/00, 19/00-19/18, G06F12/14, 15/00, H04Q7/38,
H04M1/667

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2002
Kokai Jitsuyo Shinan Koho	1971-2002	Jitsuyo Shinan Toroku Koho	1996-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 4-306760 A (Nippon Telegraph And Telephone Corp.), 29 October, 1992 (29.10.92), Full text; all drawings (Family: none)	1-32
Y	JP 9-98480 A (Sanyo Electric Co., Ltd.), 08 April, 1997 (08.04.97), Full text; all drawings (Family: none)	1-32
Y	JP 6-320891 A (Obayashi Corp.), 22 November, 1994 (22.11.94), Full text; all drawings (Family: none)	1-32

☒ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

22 July, 2002 (22.07.02)

Date of mailing of the international search report

06 August, 2002 (06.08.02)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/03789

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 4-155471 A (Oki Electric Industry Co., Ltd., NTT Data Communications Systems Corp.), 28 May, 1992 (28.05.92), Full text; Fig. 5 (Family: none)	3, 6, 17, 20
Y	JP 9-64967 A (NEC Saitama Kabushiki Kaisha), 07 March, 1997 (07.03.97), Full text; all drawings (Family: none)	31, 32
Y	JP 3-60543 A (NEC Corp.), 15 March, 1991 (15.03.91), Full text; all drawings & GB 9013610 A0 & GB 2234883 A & US 5212810 A1 & JP 2952898 B	31, 32

国際調査報告

国際出願番号 PCT/JPO2/03789

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl⁷ G06K17/00, 19/073
G06F12/14, 15/00
H04Q7/38

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int.Cl⁷ G06K17/00, 19/00-19/18
G06F12/14, 15/00
H04Q7/38, H04M1/667

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
日本国公開実用新案公報 1971-2002年
日本国登録実用新案公報 1994-2002年
日本国実用新案登録公報 1996-2002年

国際調査で使用了電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 4-306760 A(日本電信電話株式会社) 1992. 10. 29, 全文, 全図(ファミリーなし)	1-32
Y	JP 9-98480 A(三洋電機株式会社) 1997. 04. 08, 全文, 全図(ファミリーなし)	1-32
Y	JP 6-320891 A(株式会社大林組) 1994. 11. 22, 全文, 全図(ファミリーなし)	1-32

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

22. 07. 02

国際調査報告の発送日

06.08.02

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
郵便番号 100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

奥村 元宏



5N

8022

電話番号 03-3581-1101 内線 3545

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 4-155471 A(沖電気工業株式会社, エヌ・テイ・テイ・データ通信株式会社) 1992. 05. 28, 全文, 第5図 (ファミリーなし)	3, 6, 17, 20
Y	JP 9-64967 A(埼玉日本電気株式会社) 1997. 03. 07, 全文, 全図(ファミリーなし)	31, 32
Y	JP 3-60543 A(日本電気株式会社) 1991. 03. 15, 全文, 全図 & GB 9013610 A0 & GB 2234883 A & US 5212810 A1 & JP 2952898 B	31, 32